LAB University of Applied Sciences

Kameravalvontajärjestelmän toteutus

Case: Yritysympäristö

LAB-ammattikorkeakoulu
Insinööri (AMK) Tieto- ja viestintätekniikka
2026
Alex Juselius

Selvitys tekoälyn käytöstä

Tämän opinnäytetyön kirjoittaja vastaa koko työn sisällön oikeellisuudesta ja sen lopullisesta muodosta. Työssä on hyödynnetty tekoälyä rajatusti ja tarkoituksenmukaisesti siten, että sen käyttö on tukenut ideointia, rakenteen hahmottamista sekä kielellistä viimeistelyä. Tekoälyä ei ole käytetty varsinaisen sisällön tuottamiseen, menetelmävalintoihin, teknisiin laskelmiin tai johtopäätösten muodostamiseen, vaan kaikki työn analyyttinen, tekninen ja sisällöllinen kokonaisuus on kirjoittajan omaa tuotantoa.

Käytetyt kehotteet liittyivät teknisen tekstin sujuvuuteen, rakenteen vaihtoehtojen hahmotteluun sekä teoreettisen sisällön tiivistämiseen. Kirjoittaja pitää tärkeänä teknologisten työkalujen hallintaa ja niiden vastuullista hyödyntämistä osana modernia tiedonhankintaa ja raportointia. Tekoälyä on käytetty vain niissä kohdissa, joissa se tehostaa prosessia vaikuttamatta työn tutkimukselliseen kokonaisuuteen.

Tämän opinnäytetyön aitous on tarkastettu Turnitin-samankaltaisuustarkastusohjelmalla.

Tiivistelmä

Tekijä(t)	Julkaisun laji	Valmistumisaika
Alex Juselius	Opinnäytetyö, AMK	2026
	Sivumäärä	
	64	

Työn nimi

Kameravalvontajärjestelmän toteutus

Case: Yritysympäristö

Tutkinto ja koulutusala

Insinööri (AMK), tieto- ja viestintätekniikka

Toimeksiantajaorganisaatio (jos opinnäytetyöllä on toimeksiantaja)

Piilotettu

Tiivistelmä

Opinnäytetyön tavoitteena oli suunnitella ja toteuttaa yritysympäristöön IP-pohjainen kameravalvontajärjestelmä. Työ toteutettiin toiminnallisena case-toteutuksena, jossa järjestelmä suunniteltiin, asennettiin ja testattiin käytännössä. Verkkoinfrastruktuuri rakennettiin tukemaan valvontajärjestelmän luotettavaa toimintaa siltä osin kuin kameravalvonta sitä edellytti.

Toteutuksen yhteydessä suoritettiin PoE-virransyötön mitoitus, tallennuskapasiteetin ja säilytysajan laskenta sekä kaapeloinnin mittaukset. Mittaustulosten perusteella arvioitiin järjestelmän toimintavarmuutta ja teknistä soveltuvuutta kohteeseen.

Tuloksena saatiin keskitetysti hallittava ja etäkäyttöä tukeva kameravalvontajärjestelmä, joka vastaa toimeksiantajan tarpeisiin tilojen ja omaisuuden suojaamisessa. Työ osoittaa, että huolellinen tekninen mitoitus, verkkosegmentointi ja järjestelmän kokonaisvaltainen hallinta ovat keskeisiä tekijöitä yritysympäristön kameravalvonnan onnistuneessa toteutuksessa.

Asiasanat

Ip-kameravalvonta, kamerajärjestelmä, UniFi, PoE, VLAN

Abstract

Author(s)	Type of Publication	Published
Alex Juselius	Thesis, UAS	2026
	Number of Pages	
	64	

Title of Publication

Implementation of a Video Surveillance System

Case: Enterprise Environment

Degree, Field of Study

Engineer (UAS), Information and Communications Technology

Organisation of the client (if the thesis work is commissioned by another party)

Hidden

Abstract

The objective of this thesis was to design and implement an IP-based video surveillance system for an enterprise environment using the UniFi ecosystem. The work was carried out as a functional case implementation in which the system was designed, installed, and tested in practice. The network infrastructure was built to ensure reliable operation of the surveillance system to the extent required by the solution.

The implementation included Power over Ethernet (PoE) capacity sizing, storage retention calculations, and cabling measurements. The measurement results were used to evaluate system reliability and technical suitability for the target environment.

The outcome is a centrally managed and remotely accessible surveillance system that meets the client's requirements for securing premises and assets. The results demonstrate that accurate technical dimensioning, network segmentation, and integrated system management are essential factors in successful enterprise-level video surveillance implementation.

Keywords

IP video surveillance, camera system, UniFi, PoE, VLAN

Sisällys

LYHENTEET

ACR-F	Attenuation to Crosstalk Ratio Far-End, vaimennuksen ja kaukoläp-päyshäiriön suhde (vastaanottopää)
ACR-N	Attenuation to Crosstalk Ratio Near-End, vaimennuksen ja lähiläp-päyshäiriön suhde (lähettävä pää)
AI	Artificial Intelligence, tekoäly
AP	Access Point, langaton tukiasema
BR	Bitrate, videovirran bittinopeus
B-frame	Bidirectional frame, kahteen suuntaan ennustettu videoruutu
CBR	Constant Bitrate, kiinteä bittivirta
CCD	Charge-Coupled Device, kuvakenno (kamerasensori)
CMOS	Complementary Metal-Oxide-Semiconductor, kuvakenno (kamer-asensori)
DHCP	Dynamic Host Configuration Protocol, IP-osoitteiden ja verkko-asetusten automaattinen jakaminen
DSCP	Differentiated Services Code Point, IP-pakettien palveluluok-kamerkintä (QoS)
DSP	Digital Signal Processing, tässä työssä kaapelianalysaattori
EDPB	European Data Protection Board, Euroopan tietosuojaneuvosto
EN	European Norm, eurooppalainen standardi (esim. EN 50173)
FPS	Frames Per Second, videon kuvataajuus
GDPR	General Data Protection Regulation, EU:n yleinen tietosuoja-asetus
GOP	Group of Pictures, videopakkauksen ruuturyhmä (I/P/B-rakenteen jakso)
IEEE	Institute of Electrical and Electronics Engineers, standardointiorgan-isaatio
I-frame	Intra-coded frame, avainruutu (itsenäisesti koodattu ruutu)
IGMP	Internet Group Management Protocol, multicast-ryhmien hallinta
IoT	Internet of Things, verkkoon liitetyt älylaitteet
IP	Internet Protocol, verkkokerroksen osoite- ja reititysprotokolla
IP-kamera	Verkkokamera, joka välittää videokuvaa IP-verkon yli
IR	Infrared, infrapunavalo yökuvaukseen
ISP	Internet Service Provider, internet-palveluntarjoaja

LAN	Local Area Network, lähiverkko
MJPEG	Motion JPEG, videopakkaus, jossa jokainen ruutu pakataan erillisenä JPEG-kuvana
MPS	Maintain Power Signature, PoE-virransyötön ylläpidon valvontamekanismi
microSD	Muistikorttiformaatti, jota käytetään reunatallennuksessa
NEXT	Near-End Crosstalk, kaapeliparien välinen ylikuuluminen (lähettävä pää)
NVR	Network Video Recorder, IP-kameroiden tallennin
NAS	Network Attached Storage, verkkoon liitetty tallennusjärjestelmä
OSI	Open Systems Interconnection, seitsemän kerroksen viitemalli tietoliikenteelle
P-frame	Predictive frame, ennustettu videoruutu (koodaus perustuu aiempiin ruutuihin)
PD	Powered Device, PoE-virtaa vastaanottava laite
PoE	Power over Ethernet, verkkokaapelin kautta syötettävä käyttöjännite
PSE	Power Sourcing Equipment, PoE-virransyöttölaite (esim. PoE-kytkin tai -reititin)
PSNEXT	Power Sum Near-End Crosstalk, parien yhteenlaskettu ylikuuluminen
PTZ	Pan-Tilt-Zoom, kääntyvä ja zoomaava kamera
QoS	Quality of Service, verkkoliikenteen priorisointi ja hallinta
RAID	Redundant Array of Independent Disks, levyjärjestelmä
RJ45	Ethernet-verkkoliitin
RL	Return Loss, kaapeloinnin heijastusvaimennus
SAN	Storage Area Network, erillinen tallennusverkko
SIM	Subscriber Identity Module, mobiiliverkon liittymäkortti
SSID	Service Set Identifier, WLAN-verkon tunniste
TCP	Transmission Control Protocol, yhteydellinen kuljetuskerroksen protokolla
TIA	Telecommunications Industry Association, standardointiorganisaatio
UDM SE	UniFi Dream Machine Special Edition, reititin/palomuuri ja UniFi Protect -alusta UniFi-ekosysteemissä

UTP	Unshielded Twisted Pair, suojaamaton kierretty parikaapeli
VBR	Variable Bitrate, muuttuva bittivirta
VLAN	Virtual Local Area Network, virtuaalinen lähiverkko (looginen verkkosegmentointi)
WAN	Wide Area Network, laajaverkko (esim. Internet-yhteys)
Wi-Fi	Wireless Fidelity, langaton lähiverkko
WLAN	Wireless Local Area Network, langaton lähiverkko
WPA	Wi-Fi Protected Access, langattoman verkon salausprotokolla

1 Johdanto

Kameravalvonta on keskeinen osa nykyaikaista yritysten turvallisuusinfrastruktuuria. Teknologian kehittymisen myötä valvontajärjestelmät ovat laajentuneet perinteisestä videokuvan tallentamisesta kohti älykkäämpiä kokonaisuuksia, joissa hyödynnetään muun muassa tekoälyyn perustuvaa analytiikkaa, keskitettyä hallintaa ja etäkäyttömahdollisuuksia. Näiden ratkaisujen avulla yritykset voivat parantaa tilojen turvallisuutta, tehostaa valvontaa ja reagoida poikkeamatilanteisiin aiempaa nopeammin.

Yritysympäristöissä kameravalvonnan suunnittelua ja toteutusta ohjaavat yhä vahvemmin myös tietosuojaan ja lainsäädäntöön liittyvät vaatimukset. EU:n yleinen tietosuoja-asetus (GDPR) sekä kansallinen lainsäädäntö asettavat reunaehdot muun muassa henkilötietojen käsittelylle, tallenteiden säilyttämiselle ja valvonnan kohdentamiselle. Samanaikaisesti kehittyvät pilvipalvelut ja uudet älyominaisuudet tarjoavat laajempia mahdollisuuksia järjestelmien hyödyntämiseen, mutta edellyttävät huolellista suunnittelua ja sääntelyn huomioimista.

Tämän opinnäytetyön tavoitteena on suunnitella ja toteuttaa yritysympäristöön kameravalvontajärjestelmä, joka palvelee sekä pääyrityksen että vuokralaisten turvallisuus- ja seurantatarpeita. Työssä painotetaan ratkaisun skaalautuvuutta, hallittavuutta ja tietoturvallisuutta siten, että järjestelmä tukee useita käyttäjäryhmiä ja on laajennettavissa toiminnan kasvaessa. Kameravalvontajärjestelmän suunnitteluun liittyy myös lähiverkon rakenteen huomioiminen siltä osin kuin se on välttämätöntä valvontajärjestelmän toimivuuden, eriyttämisen ja tietoturvan kannalta.

Opinnäytetyö on luonteeltaan toiminnallinen ja kehittämistyyppinen. Työ perustuu yrityksen todelliseen tarpeeseen kehittää kameravalvontaratkaisu, joka on teknisesti toimiva, lainsäädännön mukainen ja yrityksen itsensä ylläpidettävissä myös tulevaisuudessa. Työn tavoitteena on tuottaa kokonaisuus, joka tukee yrityksen turvallisuutta ja toimintaa sekä tarjoaa selkeän pohjan järjestelmän jatkokehittämiselle muuttuvien vaatimusten mukaisesti.

2 Kameravalvonnan lainsäädäntö

2.1 Kameravalvontaratkaisun tausta

Tässä luvussa kuvataan kameravalvontaa koskeva keskeinen lainsäädäntö ja sitä täydentävä ohjeistus yritysympäristössä. Tarkastelu kohdistuu yrityksen omiin sisätiloihin sekä piha-alueeseen. Vuokralaisten hallinnoimiin tai yksityiskäytössä oleviin tiloihin ei kohdisteta kameravalvontaa. Valvonnan tarkoituksena on turvallisuuden ja omaisuuden suojaaminen sekä ennaltaehkäisevä valvonta.

Kamerajärjestelmässä tallennus on sekä jatkuvaa että tapahtumapohjaista. Järjestelmä kykenee teknisesti myös äänen tallentamiseen, mutta äänen käsittelyä koskevat rajoitukset huomioidaan erikseen lainsäädännön edellyttämällä tavalla. Pääsy kamerajärjestelmään on rajattu yrityksen omistajille. Opinnäytetyön toteutusvaiheessa tekijällä on ollut rajattu käyttöoikeus järjestelmään, ja nämä oikeudet luovutetaan pois työn valmistuttua.

2.2 Rikoslaki: salakatselu ja salakuuntelu

Rikoslaki (39/1889) kieltää yksityisyyttä loukkaavan salakatselun ja salakuuntelun. Salakatselulla tarkoitetaan teknisellä laitteella tapahtuvaa oikeudetonta katselua tai kuvaamista tilanteissa, joissa henkilö oleskelee kotirauhan suojaamassa tai muussa yksityisyyttä korostavassa paikassa. Tällaisia tiloja ovat esimerkiksi asunnot, wc- ja pesutilat sekä pukeutumistilat.

Salakuuntelu puolestaan tarkoittaa keskustelun tai muun äänen kuuntelemista tai tallentamista ilman lupaa tilanteessa, jossa puhujalla ei ole syytä olettaa ulkopuolisen kuulevan. Yksityisen puheen luvaton tallentaminen on rangaistavaa riippumatta siitä, tapahtuuko se tallennuslaitteen avulla vai reaaliaikaisesti. Kameravalvonnan yhteydessä tämä merkitsee sitä, että äänen tallentaminen on lähtökohtaisesti kielletty, ellei siihen ole erikseen laissa säädettyä ja välttämätöntä perustetta. (Rikoslaki 39/1889.)

2.3 Työpaikan kameravalvonta ja henkilötietolain periaatteet

Laki yksityisyyden suojasta työelämässä (759/2004) määrittelee ne edellytykset, joilla kameravalvontaa voidaan käyttää työpaikalla. Valvonnan sallittuja tarkoituksia ovat muun muassa työntekijöiden turvallisuuden varmistaminen, omaisuuden suojaaminen sekä tuotantoprosessien asianmukaisen toiminnan seuraaminen. Kameravalvontaa ei kuitenkaan saa käyttää yksittäisen työntekijän tai työntekijäryhmän seurantaan eikä työtehon valvontaan. Lisäksi valvonta on kielletty sosiaalitiloissa ja muissa yksityisyyttä korostavissa tiloissa.

Ennen GDPR:n voimaantuloa henkilötietojen käsittelyä ohjasi henkilötietolaki (523/1999), jonka keskeisiä periaatteita olivat tarkoitussidonnaisuus, tarpeellisuus ja tietojen suojaaminen. Nämä periaatteet ovat sittemmin siirtyneet osaksi voimassa olevaa tietosuojasääntelyä. Työelämän tietosuojasääntely muodostuu nykyisin työelämän yksityisyyden suojasta annetun lain, EU:n yleisen tietosuoja-asetuksen sekä kansallisen tietosuojalain kokonaisuudesta, jota valvovat yhteistyössä työsuojeluviranomaiset ja tietosuojavaltuutettu. (Tietosuojavaltuutetun toimisto 2020.)

2.4 GDPR ja tietosuojalaki kameravalvonnassa

Kameravalvonta, jossa käsitellään tunnistettavia kuvia tai ääntä, on henkilötietojen käsittelyä ja kuuluu EU:n yleisen tietosuoja-asetuksen (GDPR) soveltamisalaan. Rekisterinpitäjänä toimii taho, joka määrittelee kameravalvonnan tarkoitukset ja keinot. Kameravalvonnan oikeusperusteena on useimmiten rekisterinpitäjän oikeutettu etu, jonka toteutuminen edellyttää etujen punnintaa suhteessa rekisteröityjen perusoikeuksiin. (EU 2016/679.)

Suomen tietosuojalaki (1050/2018) täydentää GDPR:ää kansallisessa soveltamisessa ja täsmentää muun muassa viranomaisvalvontaa sekä erityisten henkilötietoryhmien käsittelyä. Tietosuojavaltuutetun mukaan kameravalvonta on aina henkilötietojen käsittelyä riippumatta siitä, tallennetaanko kuvaa vai ei. Myös pelkkä reaaliaikainen kameravalvonta kuuluu tietosuojasääntelyn piiriin. Tallenteita saa säilyttää vain niin kauan kuin se on käsittelyn tarkoituksen kannalta tarpeellista. (Tietosuojavaltuutetun toimisto 2023.)

2.5 AI-laki ja biometrinen tunnistaminen kameravalvonnassa

Euroopan unionin tekoälyasetus (AI Act 2024/1689) luokittelee tekoälyjärjestelmät eri riskiluokkiin ja asettaa tiukkoja rajoituksia erityisesti korkean riskin ja kiellettyihin käyttötapoihin kuuluville järjestelmille. Kameravalvonnan kannalta keskeisiä ovat kiellot, jotka koskevat biometriseen tunnistamiseen ja kategorisointiin perustuvia järjestelmiä sekä reaaliaikaista etäbiometristä tunnistusta julkisissa tiloissa. Lisäksi asetus kieltää biometrisista tiedoista arkaluonteisten ominaisuuksien päättelemisen sekä työntekijöiden tunteiden analysoinnin, koska näiden katsotaan muodostavan merkittävän perusoikeusriskin ja mahdollistavan syrjiviä tai suhteettomia valvontakäytäntöjä. (EU 2024/1689.)

EU:n yleinen tietosuoja-asetus (GDPR) määrittelee biometriset tiedot erityisiin henkilötietoryhmiin kuuluviksi tiedoiksi, joiden käsittely on lähtökohtaisesti kielletty. Työelämässä biometristen tietojen käsittely edellyttää poikkeuksellista oikeusperustetta sekä tiukkojen suojatoimien toteuttamista, eikä pelkkä työnantajan intressi riitä käsittelyn oikeuttamiseksi. Kameravalvonnassa tämä tarkoittaa sitä, että tunnistamiseen tai yksilöivään analyysiin

perustuvia toimintoja ei voida ottaa käyttöön ilman nimenomaista ja laillista perustetta. (EU 2016/679.)

Euroopan tietosuojaneuvoston (EDPB) antama ohjeistus täydentää lainsäädäntöä ja täsmentää tietosuojaperiaatteiden soveltamista kameravalvonnassa. Ohjeistuksessa korostetaan erityisesti henkilötietojen minimointia, rekisteröityjen asianmukaista ja läpinäkyvää informointia sekä käyttöoikeuksien ja lokituksen huolellista hallintaa. Näiden periaatteiden tavoitteena on varmistaa, että kameravalvontajärjestelmät toteutetaan oikeasuhtaisesti ja siten, että rekisteröityjen oikeudet ja yksityisyyden suoja toteutuvat käytännössä. (EDPB 2019.)

3 Tietoverkot kameravalvonnan toimintaympäristönä

3.1 OSI-malli teoreettisena viitekehyksenä

Tässä työssä OSI-mallia hyödynnetään teoreettisena viitekehyksenä IP-pohjaisen kameravalvontajärjestelmän tietoverkollisen perustan tarkastelussa. Tarkastelu rajataan mallin kolmeen alimpaan kerrokseen: fyysiseen kerrokseen, tiedonsiirtokerrokseen ja verkkokerrokseen. Näissä kerroksissa käsitellään siirtotien ominaisuuksia, paikallisen tiedonsiirron mekanismeja sekä loogisen osoitteistuksen ja reitityksen periaatteita. Ylempien OSI-kerrosten toiminnallisuudet rajataan tarkastelun ulkopuolelle, koska työn painopiste on tietoverkon rakenteellisessa ja toiminnallisessa perustassa.

Open Systems Interconnection -malli (OSI-malli) on kerroksellinen viitekehys, jonka avulla tietoliikennejärjestelmien toiminta voidaan jäsentää loogisiin kokonaisuuksiin. Malli jakaa tietoliikenteen seitsemään kerrokseen, joista kukin vastaa omasta toiminnallisesta osa-alueestaan ja rajapinnastaan suhteessa ylempiin ja alempiin kerroksiin. OSI-mallin tarkoituksena ei ole määritellä yksittäisiä protokollia tai toteutustapoja, vaan tarjota yleinen ja standardoitu tapa kuvata tietoliikennejärjestelmien rakennetta ja toimintaa riippumatta käytetystä teknologiasta (ISO/IEC 7498-1).

3.2 Fyysinen kerros (Layer 1): kaapelointi ja Power over Ethernet

OSI-mallin fyysinen kerros määrittelee tiedonsiirron sähköiset ja mekaaniset ominaisuudet, kuten siirtotien rakenteen, liitännät ja signaalitasot. Fyysisen kerroksen tehtävänä on mahdollistaa tiedon siirto siirtotietä pitkin siten, että ylemmät kerrokset voivat toimia riippumatta siirtotien teknisistä yksityiskohdista (ISO/IEC 7498-1). Verkkopohjaisissa kameravalvontajärjestelmissä fyysisen kerroksen toiminta on merkityksellistä, koska sekä videodatan siirto että virransyöttö voivat hyödyntää samaa fyysistä siirtotietä (Li & Zhu 2020).

Power over Ethernet (PoE) on tekniikka, jossa sekä data että tasavirta siirretään samaa Ethernet-pohjaista kierrettyä parikaapelia pitkin. PoE-järjestelmässä virransyöttö tapahtuu verkon virransyöttölaitteen (Power Sourcing Equipment, PSE) kautta, ja virtaa vastaanottavaa laitetta kutsutaan powered device -laitteeksi (PD). PoE mahdollistaa kameroiden asentamisen ilman erillistä sähkökaapelointia, mikä vähentää asennusten monimutkaisuutta ja helpottaa järjestelmän hallintaa erityisesti laajoissa kameravalvontakokonaisuuksissa (Li & Zhu 2020).

PoE-järjestelmän toiminta perustuu PSE- ja PD-laitteiden väliseen tunnistus- ja neuvotteluprosessiin, jonka avulla varmistetaan, että virtaa syötetään ainoastaan PoE-yhteensopiville laitteille. Virransyötön aikana järjestelmä valvoo maintain power signature (MPS) -

mekanismin avulla, että PD-laite kuluttaa vähimmäisvirtaa osoittaakseen olevansa edelleen kytketty ja toimintakunnossa. Mikäli MPS-ehto ei täyty riittävän pitkään, PSE tulkitsee PD-laitteen irrotetuksi ja katkaisee virransyötön turvallisuussyistä (Li & Zhu 2020).

PoE-tekniikkaa on standardoitu useisiin luokkiin ja tyyppeihin, jotka määrittävät käytettävien johtoparien lukumäärän sekä suurimman sallitun tehon PSE- ja PD-laitteille. Varhaisemmat PoE-standardit hyödyntävät kahta johtoparia, kun taas uudemmissa standardeissa virransyöttö voidaan toteuttaa kaikilla neljällä parilla suurempien tehotarpeiden mahdollistamiseksi. Taulukko 1 esittää PoE-luokat, -tyypit ja standardit sekä niihin liittyvät tehorajat.

	Type 3 PoE (802.3bt)							Type 4 PoE (802.3bt)
	Type 1 PoE (802.3af)			Type 2 PoE (802.3at)				
# of Pairs	2-pair only (Type 1 & 2)				Always 4-pairs			
	2-pair or 4 pair (Type 3 & 4)							
Class	Class 1:	Class 2:	Class 3:	Class 4:	Class 5:	Class 6:	Class 7:	Class 8:
PSE	4 W	7W	15.4 W	30 W	45 W	60 W	75 W	90 W
PD	3.84 W	6.49 W	13 W	25.5 W	40 W	51 W	62 W	73.3 W

Taulukko 1. PoE-luokat, -tyypit ja standardit. Lähde: Fluke Networks.

Kameravalvontajärjestelmissä virrankulutus ei ole vakio, vaan se voi vaihdella esimerkiksi valaistusolosuhteiden, infrapunavalojen ja muiden lisätoimintojen käytön mukaan. Tällaisissa tilanteissa virrankulutus voi ajoittain laskea hyvin alhaiselle tasolle, jolloin MPS-vaatimusten täyttyminen korostuu. Tämän vuoksi virransyötön hallinta fyysisellä kerroksella liittyy järjestelmän luotettavaan toimintaan, erityisesti tilanteissa, joissa kamerat toimivat valmius- tai alhaisen kuormituksen tilassa (Li & Zhu 2020).

Edellä kuvattu tunnistus- ja neuvotteluprosessi koskee standardoituja IEEE 802.3 -pohjaisia PoE-ratkaisuja. Lisäksi on olemassa passiivisia PoE-toteutuksia, joissa jännite, esimerkiksi 24 voltin tasavirta, syötetään Ethernet-kaapeliin ilman laitteen tunnistusta tai tehonneuvottelua. Passiivinen PoE ei sisällä suojausmekanismeja vääränlaista kuormaa vastaan, minkä vuoksi yhteensopimaton laite tai mittalaite voi vaurioitua, jos jännitteellinen kaapeli kytketään laitteeseen ilman tietoa virransyötöstä (Ubiquiti Inc. 2026).

3.3 Tiedonsiirtokerros (Layer 2): Ethernet ja VLAN-segmentointi

OSI-mallin tiedonsiirtokerros vastaa tiedon siirtämisestä paikallisessa verkossa fyysisen siirtotien yli. Kerros määrittelee kehystämisen periaatteet, laitteiden tunnistamisen MAC-

osoitteiden avulla sekä virheiden havaitsemisen ja paikallisen tiedonsiirron hallinnan. Tiedonsiirtokerroksen tehtävänä on varmistaa, että fyysisen kerroksen kautta siirretty data välittyy luotettavasti saman lähiverkon laitteiden välillä ennen liikenteen mahdollista välittämistä ylemmille kerroksille (ISO/IEC 7498-1).

Tiedonsiirtokerroksella Ethernet-verkot hyödyntävät Media Access Control (MAC) -osoitteita, jotka ovat verkkoliitäntäkohtaisia ja yksilöllisiä. Ethernet-kehysten välitys perustuu näihin MAC-osoitteisiin, ja Ethernet-kytkimet välittävät sekä unicast- että broadcast-kehyksiä lähiverkon sisällä. Ethernet-tason broadcast-liikenne käyttää erityistä MAC-osoitetta (FF:FF:FF:FF:FF:FF) ja tavoittaa kaikki saman broadcast-domainin laitteet. Layer 2 -tason broadcast-liikenne ei ylitä reitittimiä, sillä reitittimet eivät välitä Ethernet-broadcast-kehyksiä ja siten erottavat broadcast-domainit toisistaan (Elsevier 2026).

Virtual Local Area Network (VLAN) on tiedonsiirtokerroksen tekniikka, jonka avulla fyysinen lähiverkko voidaan jakaa useisiin loogisiin verkkoihin. Kukin VLAN muodostaa oman erillisen Ethernet-tason broadcast-alueensa, jossa samaan VLANiin kuuluvat laitteet voivat kommunikoida keskenään, mutta eri VLANeihin kuuluvat laitteet eivät ilman verkkokerroksen reititystä voi vaihtaa tietoa. VLAN-segmentoinnin avulla voidaan rajoittaa broadcast-liikennettä, parantaa verkon suorituskykyä ja lisätä tietoturvaa eristämällä kameravalvontajärjestelmän liikenne muusta lähiverkosta (Huawei Technologies 2024).

3.4 Verkkokerros (Layer 3): IP-osoitteistus, aliverkot ja IP-liikenteen jakelumallit

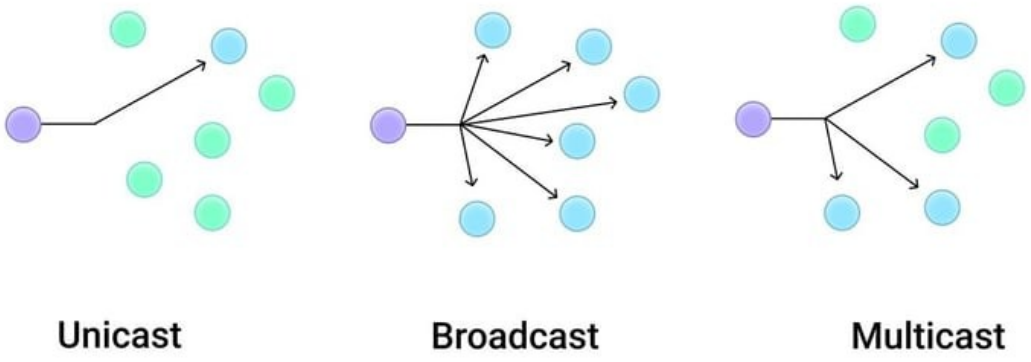
OSI-mallin verkkokerros vastaa loogisesta osoitteistuksesta sekä liikenteen reitityksestä eri verkkojen välillä. Verkkokerroksen tehtävänä on mahdollistaa tiedonsiirto useiden erillisten lähiverkkojen yli siten, että datapaketit voidaan tunnistaa, osoittaa ja ohjata kohti oikeaa kohdeverkkoa riippumatta fyysisestä siirtotiestä tai paikallisesta tiedonsiirtotekniikasta (ISO/IEC 7498-1). IP-pohjaisissa verkoissa nämä toiminnot toteutuvat Internet Protocol -protokollan avulla (IETF 1981).

IP-verkossa jokaiselle päätelaitteelle määritellään yksilöllinen IP-osoite, jonka avulla laite voidaan tunnistaa ja tavoittaa verkossa. Osoitteistus voidaan jakaa aliverkkoihin etuliitepohjaisen osoitteistuksen avulla, jolloin määritellään, mitkä osoitteet kuuluvat samaan loogiseen verkkoon ja mitkä edellyttävät liikenteen välittämistä reitittimen kautta toiseen verkkoon. Reititys perustuu reitittimen ylläpitämään reititystauluun, jonka avulla datapaketit ohjataan oikeaan verkkoon silloin, kun kohdeosoite ei kuulu lähettäjän omaan aliverkkoon (IETF 1981).

Vaikka sekä tiedonsiirtokerroksella että verkkokerroksella esiintyy broadcast-liikennettä, kyseessä ovat eri kerrosten mekanismit. Ethernet-broadcast toimii MAC-tasolla paikallisessa

lähiverkossa ja on sidottu tiedonsiirtokerroksen broadcast-domainiin. IP-verkoissa broadcast perustuu verkkokerroksen osoiterakenteeseen, ja IPv4-broadcast-liikenne rajoittuu tiettyyn aliverkkoon. IP-broadcast-paketteja ei välitetä reitittimien kautta, vaan ne jäävät paikalliseen aliverkkoon (Elsevier 2026b).

IP-pohjaisissa verkoissa tiedonsiirto voidaan toteuttaa eri jakelumalleilla sen mukaan, kenelle data on tarkoitettu. Keskeiset IP-jakelumallit ovat unicast, broadcast ja multicast, jotka eroavat toisistaan vastaanottajien määrän ja verkkoon kohdistuvan kuormituksen näkökulmasta (Lammle 2017). Jakelumallien periaatteellinen ero on havainnollistettu kuviossa 1.



Kuvio 1. Broadcast-, unicast- ja multicast-liikenteen periaatteellinen ero. Lähde: TeleDynamics 2023.

Unicast-liikenne on IP-verkoissa yleisin jakelutapa, jossa tiedonsiirto tapahtuu yhdeltä lähettäjältä yhdelle yksilöidylle vastaanottajalle IP-osoitteen perusteella. Unicast-paketit on aina osoitettu yksittäiselle kohdelaitteelle, ja ne voivat kulkea useiden reitittimien kautta osana IP-verkkoa (Microsoft 2009). Kameravalvontajärjestelmissä unicast-liikennettä syntyy tyypillisesti tilanteissa, joissa yksittäinen käyttäjä tarkastelee yhden IP-kameran live-kuvaa.

Broadcast-liikenteessä IP-paketti lähetetään kaikille saman aliverkon laitteille. Broadcast-liikenne ei ylitä reitittimiä ja runsas käyttö voi heikentää verkon suorituskykyä erityisesti laajoissa lähiverkoissa (Lammle 2017).

Multicast-liikenteessä lähettäjä välittää datapaketteja multicast-ryhmälle, ja vain ryhmään liittyneet laitteet vastaanottavat liikenteen. Multicast mahdollistaa saman videovirran jakamisen useille vastaanottajille ilman useita rinnakkaisia unicast-yhteyksiä, mikä vähentää verkon kokonaiskuormitusta (Lammle 2017).

IP-osoitteiden hallinta voidaan toteuttaa joko staattisesti tai dynaamisesti. Vaikka Dynamic Host Configuration Protocol (DHCP) on OSI-mallin mukaisesti sovelluskerroksen

protokolla, se liittyy toiminnallisesti verkkokerrokseen, koska sen tehtävänä on jakaa IP-osoitteita ja muita verkkokerroksen toiminnan kannalta keskeisiä asetuksia, kuten aliverkon peite ja oletusyhdyskäytävä. DHCP noudattaa asiakas–palvelinmallia, jossa DHCP-palvelin jakaa verkkoon liitettäville laitteille tarvittavat verkkoasetukset. Dynaaminen osoitteiden allokointi helpottaa verkon hallintaa ja mahdollistaa laitteiden liittämisen verkkoon ilman manuaalista konfigurointia (IETF 1997).

3.5 Liikenteen hallinta OSI-kerrosten rajapinnassa: QoS-periaatteet

Quality of Service (QoS) viittaa mekanismeihin, joilla verkkoliikenteen käsittelyä voidaan ohjata tilanteissa, joissa verkkokapasiteetti on rajallinen. OSI-mallin näkökulmasta QoS ei sijoitu yksiselitteisesti yhteen kerrokseen, vaan se hyödyntää useiden kerrosten toimintoja erityisesti tiedonsiirtokerroksen ja verkkokerroksen rajapinnassa, kuten liikenteen luokittelua ja pakettien merkintää (Fortinet 2026).

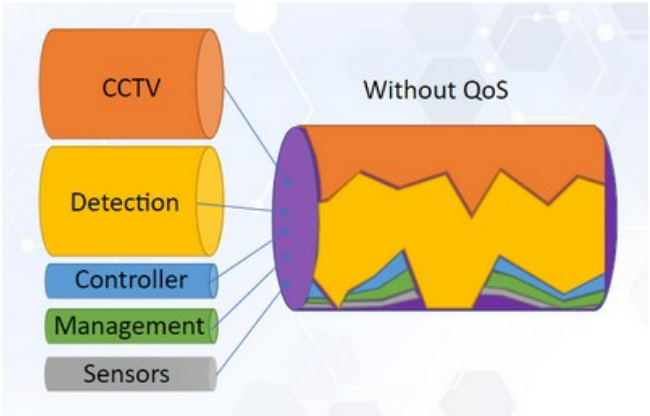
QoS-mekanismien avulla liikennettä voidaan priorisoida sovelluksen tai liikennevirran ominaisuuksien perusteella. Tämä on erityisen merkityksellistä videopohjaisissa järjestelmissä, joissa viive, viiveen vaihtelu ja pakettihävikki vaikuttavat kuvan laatuun. QoS:n avulla voidaan hallita jonotusta, varata kaistanleveyttä ja määrittää pakettien käsittelyjärjestys ruuhkatilanteissa (Fortinet 2026).

QoS liittyy keskeisesti suorituskykymittareihin, kuten viiveeseen (delay), pakettihävikkiin (loss) ja viiveen vaihteluun (jitter). Näiden mittareiden hallinta on osa aikaherkkien sovellusten liikenteen käsittelyä. Liikenteen muotoilu, jonotusalgoritmit sekä pakettien merkitseminen esimerkiksi DSCP-mekanismien avulla ovat keskeisiä QoS-toteutuksen osia (Fortinet 2026).

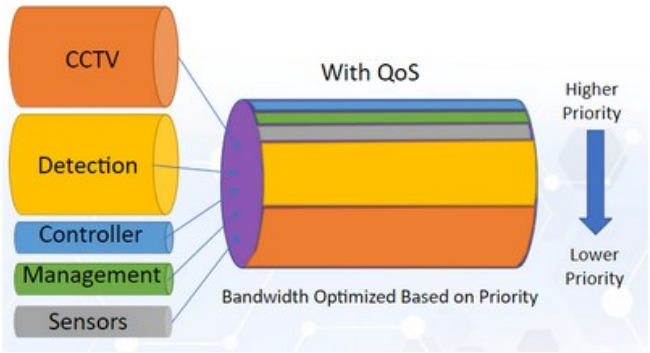
Liikenteen priorisoinnin ero havainnollistettu kuviossa 2.

Traffic With and Without QoS

As the volume of data increases towards 100% utilization, the potential for loss of data increases exponentially. In this image all data is trying to fit through the pipe. In the process, some critical data is lost.



With QoS, critical traffic is protected, and passes through without loss as shown below.



Kuvio 2. Liikenteen priorisointi QoS-mekanismien avulla. Mukaillen: EtherWAN 2023

4 IP-kameravalvonta

4.1 IP-Kamera ja laitetyypit

IP-kamera on valvontalaite, joka muuntaa ja käsittelee kameran tuottaman kuvan digitaaliseksi, pakkaa (koodaa) videon kameran sisällä ja välittää videoinformaation digitaalisesti verkon yli joko langallista tai langatonta yhteyttä käyttäen esimerkiksi tietokoneelle tai muulle vastaavalle päätelaitteelle. Lubobya ym. kuvaavat IP-kameran koostuvan tyypillisesti optiikasta sekä kuvan muodostukseen ja käsittelyyn liittyvistä komponenteista, kuten kuvakennosta (CCD tai CMOS), analogia–digitaalimuuntimesta ja digitaalisesta signaaliprosessoinnista (DSP). Näiden avulla kuva muodostetaan, muunnetaan digitaaliseen muotoon ja koodataan ennen verkkoon siirtoa, mikä erottaa IP-kameran perinteisestä analogisesta kamerasta erityisesti tiedonsiirron ja järjestelmäintegraation näkökulmasta. (Lubobya ym. 2018.)

Kameralaitetyypit

IP-kameroita on useita rakenteellisia ja käyttötarkoituksen mukaan eriytyviä tyyppejä. Lubobya ym. mainitsevat esimerkkeinä dome-, box-, bullet-, covert- ja PTZ-kamerat (pan–tilt–zoom) sekä näihin rinnastettavat muut toteutukset. Osa edellä mainituista tyypeistä voi sisältää myös Wi-Fi-toiminnallisuuden, jolloin kamera voidaan liittää verkkoon langattomasti kohteen asennus- ja infrastruktuurirajoitteiden mukaan. Kameratyypin valinta kytkeytyy käytännössä siihen, millainen fyysinen rakenne, asennustapa ja ohjausominaisuudet (esimerkiksi PTZ:n mekaaninen suuntaus ja zoom) soveltuvat valvottavaan ympäristöön ja tavoiteltuun käyttötapaan. (Lubobya ym. 2018.)

Kuvassa 1 on esitelty yleisimpiä kameroita.

Kuva 1. Tekoälyn luomat IP-kameratyypit: bullet, dome, turret ja PTZ

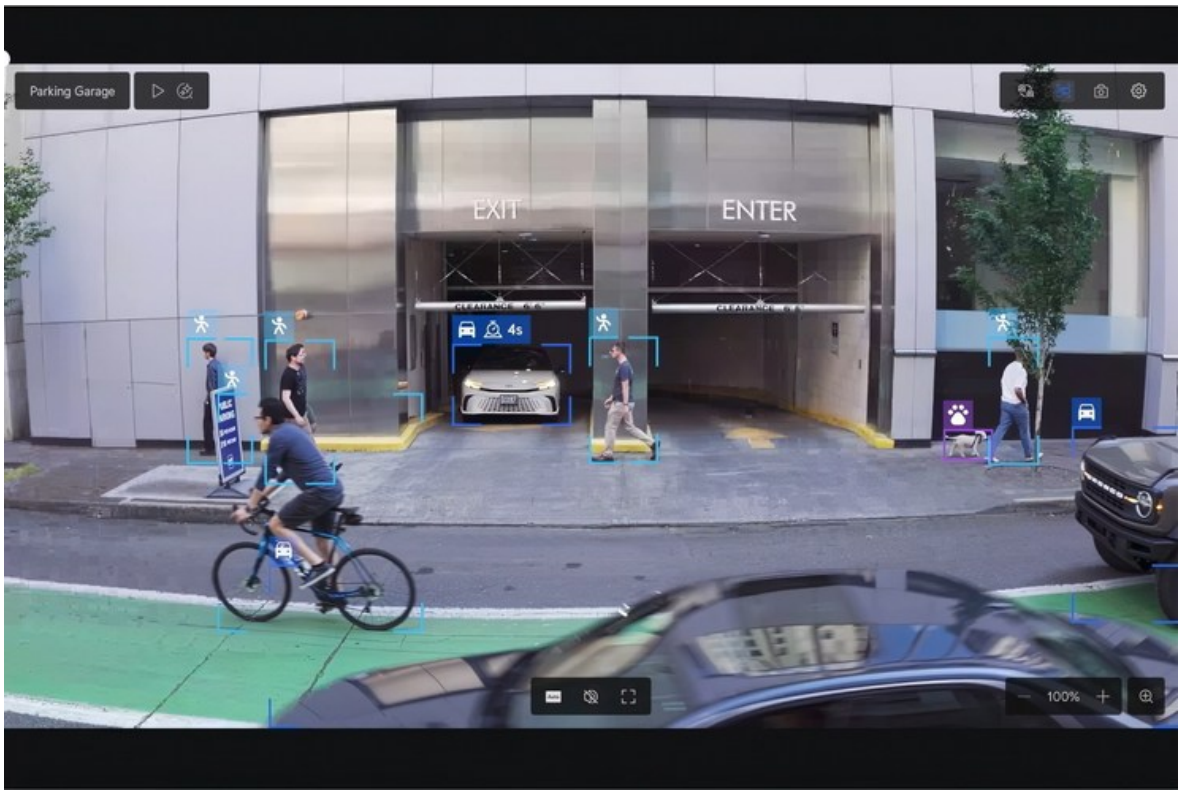
4.2 Tapahtumapohjainen tallennus ja älykkäät tunnistukset

Perinteisen jatkuvan tallennuksen rinnalle on kehittynyt tapahtumapohjainen tallennus, jossa videomateriaalin tallennus, luokittelu ja hälytysten muodostaminen perustuvat ennalta määriteltyihin tapahtumiin. Tällaisia tapahtumia voivat olla esimerkiksi henkilön tai ajoneuvon tunnistaminen, määritellyn alueen tai linjan ylittäminen sekä poikkeavien äänien havaitseminen. Tapahtumapohjainen lähestymistapa vähentää tallennettavan aineiston määrää ja nopeuttaa olennaisten tilanteiden löytämistä suurista videomassoista. (Ubiquiti 2025.)

Tapahtumapohjainen tallennus perustuu tekoälyavusteisiin tunnistuksiin, jotka analysoivat videokuvaa ja ääntä reaaliaikaisesti. Järjestelmä kykenee luokittelemaan kohteita, kuten henkilöitä ja ajoneuvoja, sekä tunnistamaan tarkempia piirteitä, kuten kasvoja, rekisterikilpiä tai ajoneuvotyyppejä. Lisäksi järjestelmä tukee ääneen perustuvia tunnistuksia, kuten puheen tai lasin rikkoutumisen havaitsemista, mikä laajentaa valvonnan ulottuvuutta pelkän kuvapohjaisen analyysin ulkopuolelle. (Ubiquiti 2025.)

Älykkäiden tunnistusten keskeinen tekninen periaate UniFi Protect -järjestelmässä on reunalaskenta (edge AI). Analyysi suoritetaan paikallisesti joko suoraan kamerassa tai erillisissä tekoälylaitteissa, kuten AI Port- tai AI Key -yksiköissä, ilman että videovirtaa siirretään pilvipalveluihin analysoitavaksi. Tämä parantaa tietosuojaa, pienentää viiveitä ja vähentää verkon kuormitusta verrattuna pilvipohjaisiin analyysiratkaisuihin. (Ubiquiti 2025.)

Tapahtumapohjaiset tunnistukset eivät rajoitu pelkkään tallennukseen, vaan ne integroituvat osaksi järjestelmän muita toimintoja. Tunnistustapahtumia voidaan hyödyntää hakutoiminnoissa, tapausraporttien muodostamisessa sekä automaatioissa, joissa havaitut tapahtumat käynnistävät ennalta määriteltyjä toimintoja, kuten valaistuksen ohjauksen tai muiden järjestelmien aktivoinnin. Näin älykkäät tunnistukset tukevat kameravalvontaa paitsi turvallisuuden valvonnassa myös tapahtumien tehokkaassa jälkikäsittelyssä ja järjestelmän operatiivisessa käytössä. (Ubiquiti 2025.) Esimerkki tapahtumapohjaisesta tunnistuksesta kuvassa 2.



Kuva 2. Tapahtumapohjainen tunnistus UniFi Protect -järjestelmässä. Lähde: Ubiquiti 2024.

4.3 Videovirta ja bittinopeuden muodostuminen

IP-kameran tuottama videovirta on jatkuva datavirta, joka sisältää kuvan lisäksi mahdollisen äänen sekä ohjaus- ja metatietoja. Videovirran hetkellinen koko eli tarvittava kaistanleveys (bandwidth) määräytyy siitä, kuinka paljon dataa järjestelmä tuottaa ja siirtää sekunnissa. Kaistanleveys on keskeinen mitoitusparametri, koska se vaikuttaa sekä verkkoinfrastruktuurin kuormitukseen että tallennusjärjestelmän kapasiteetti- ja retentiolaskelmiin. (Fortinet 2025.)

Fortinetin esittämän mallin mukaan IP-valvontakameran kaistanleveyteen vaikuttaa kuusi päätekijää: (1) käytetty videokoodekki ja sen pakkaustapa, (2) tavoiteltu kuvanlaatuprofiili, (3) kuvattavan näkymän monimutkaisuus ja liikkeen määrä (scene complexity), (4) videon

resoluutio, (5) kuvanopeus (fps) sekä (6) samanaikaisesti tuotettavien ja katseltavien videovirtojen määrä (kameroiden ja katselijoiden lukumäärä). Tekijät eivät vaikuta toisistaan riippumatta: esimerkiksi korkea resoluutio ja suuri kuvanopeus lisäävät datamäärää, ja monimutkainen tai kohinainen kuva heikentää pakkauksen tehokkuutta, jolloin tarvittava bittinopeus kasvaa. (Fortinet 2025.)

Mallin käytännön merkitys suunnittelussa on se, että “kameran bittinopeus” ei ole kiinteä yksittäinen arvo, vaan asetuksista ja kuvaolosuhteista riippuva vaihteluväli. Tästä syystä verkon ja tallennuksen mitoitus tehdään tyypillisesti arvioiduilla keskimääräisillä bittivirroilla ja varmistetaan käytännön havainnoilla käyttöönoton jälkeen. Näin verkon käsittely rajataan opinnäytetyössä niihin kohtiin, jotka ovat kameravalvonnan toimivuuden ja tallennusvarmuuden kannalta olennaisia. (Fortinet 2025.)

4.4 Videokoodekit

Videokoodekki määrittää, miten videokuva pakataan siirtoa ja tallennusta varten. Fortinetin Whitepaperin mukaan MJPEG, H.264 ja H.265 ovat valvontakameroissa tyypillisiä vaihtoehtoja, mutta niiden kaistanleveysvaikutus poikkeaa selvästi toisistaan. MJPEG toteuttaa pakkauksen “kuva kuvalta” siten, että jokainen ruutu pakataan itsenäisenä JPEG-kuvana. Tämän seurauksena MJPEG kasvattaa bittivirtaa merkittävästi verrattuna nykyaikaisiin ennustepohjaisiin koodekkeihin, koska ruutujen välistä redundanssia ei hyödynnetä tehokkaasti. (Fortinet 2025.)

H.264:n perusidea on, että täysiä avainruutuja (I-frame) lähetetään tietyin välein ja niiden väliin jäävät ruudut koodataan pääasiassa muutoksina edellisiin ja/tai seuraaviin ruutuihin nähden (P- ja B-ruudut). Tätä I/P/B-ruutujen toistuvaa rakennetta kutsutaan GOP:ksi (group of pictures), ja I-ruutujen väli vaikuttaa bittivirran käyttäytymiseen: tiheämmät I-ruudut parantavat kuvan uudelleendekoodauksen “uudelleenkäynnistyvyyttä”, mutta lisäävät tyypillisesti streamin kokoa, kun taas harvemmat I-ruudut pienentävät keskimääräistä bittivirtaa mutta voivat tehdä katkoksista ja hakemisesta herkempiä. (Fortinet 2025.)

H.265 on H.264:n seuraaja, jonka tavoitteena on parempi pakkaustehokkuus: sama kuvanlaatu voidaan saavuttaa pienemmällä bittivirralla, mikä on hyödyllistä erityisesti korkearesoluutioisessa videossa. Whitepaper korostaa kuitenkin, että H.265:n käyttö voi rajoittua yhteensopivuuteen ja laitteistotukeen liittyviin tekijöihin (esimerkiksi päätelaitteiden toisto- ja dekoodaustuki), minkä vuoksi H.264 säilyy monissa ympäristöissä laajasti käytettynä vaihtoehtona. (Fortinet 2025.)

4.5 Bitrate-mallit: CBR ja VBR

Bittivirran hallintamalli määrittää, pysyykö kameran tuottama bittivirta tasaisena vai muuttuuko se tilanteen mukaan. VBR (variable bitrate) pyrkii säilyttämään kuvanlaadun tasaisempana antamalla bittivirran vaihdella kuvan sisällön mukaan. Tämä sopii tilanteisiin, joissa kuvassa on vaihtelevasti liikettä ja yksityiskohtia: rauhallisessa näkymässä bittivirta voi laskea, ja tapahtumien aikana se voi kasvaa. Haittapuolena on, että hetkelliset piikit voivat kuormittaa verkkoa ja kuluttaa tallennustilaa ennakoitua nopeammin, jolloin mitoitus perustuu helpommin arvioihin ja varmuusmarginaaleihin. (Fortinet 2025.)

CBR (constant bitrate) pitää bittivirran tavoitetason tasaisempana. Kun kuvassa tapahtuu enemmän muutoksia, koodekki lisää pakkausta pysyäkseen asetetussa bittinopeudessa, mikä voi näkyä kuvanlaadun heikkenemisenä ja pakkausartefakteina. CBR helpottaa erityisesti verkon ja tallennuksen ennustettavaa mitoitusta, koska kameran kaistanleveyden yläraja on hallitumpi, mutta se tekee kuvanlaadusta herkemmän monimutkaisille näkymille ja ruuhkatilanteille. (Fortinet 2025.)

Jos lähiverkossa on hyvin kapasiteettia ja tavoitteena on paras kuvanlaatu, VBR on usein perusteltu valinta, kun taas kaistanleveyden ollessa rajallinen tai mitoituksen ennustettavuuden ollessa ensisijaista CBR tukee hallittavampaa kokonaisuutta. Valinta tehdään lopulta kohdeympäristön, kamerapisteiden kriittisyyden ja tallennus-/katselutarpeiden perusteella. (Fortinet 2025.)

4.6 Tallennusmallit (NVR, Edge, NAS)

IP-pohjaisissa kameravalvontajärjestelmissä videodatan tallennus voidaan toteuttaa useilla eri arkkitehtuureilla. Yleisimmät tallennusmallit ovat keskitetty tallennus verkkotallentimeen (Network Video Recorder, NVR), kamerakohtainen reunatallennus (edge storage) sekä erilliseen verkkoon liitetty tallennusjärjestelmä (Network Attached Storage, NAS).

NVR-pohjainen tallennus

NVR-pohjaisessa tallennusmallissa kaikki kameroiden tuottamat videovirrat välitetään keskitetylle tallennuspalvelimelle, jossa video tallennetaan paikallisille kiintolevyille. Axisin IP-Surveillance Design Guide -julkaisun mukaan tämä malli on yleisin ratkaisu pienissä ja keskisuurissa IP-kameravalvontajärjestelmissä, koska se mahdollistaa tallennuksen, käyttäjäoikeuksien ja tallenteiden hallinnan yhden järjestelmän kautta (Axis Communications, 2007).

Keskitetyn tallennuksen etuna on selkeä hallintamalli: tallennusasetukset, säilytysajat, käyttäjäroolit ja tapahtumahaut voidaan toteuttaa yhden käyttöliittymän kautta. Tämä vähentää

järjestelmän operatiivista monimutkaisuutta ja tukee valvontajärjestelmän käyttöä myös eiteknisten käyttäjien toimesta. Haittapuolena on keskitetyn tallentimen muodostama yksittäinen vikapiste, ellei järjestelmään ole toteutettu vikasietoisuutta esimerkiksi RAID-ratkaisujen tai varmuuskopioinnin avulla (Axis Communications, 2007).

Reunatallennus (Edge storage)

Reunatallennuksessa videodata tallennetaan suoraan kameran omaan muistiin, tyypillisesti microSD-kortille, tai muuhun verkon reunalla sijaitsevaan tallennuslaitteeseen. Axis Communicationsin Edge storage -white paperin mukaan reunatallennus parantaa järjestelmän toimintavarmuutta erityisesti tilanteissa, joissa verkkoyhteys on epävakaa, rajallinen tai tilapäisesti poissa käytöstä (Axis Communications, 2021).

Reunatallennusta käytetään usein täydentävänä ratkaisuna keskitetyn tallennuksen rinnalla. Tällöin kamera tallentaa videon paikallisesti verkkohäiriön aikana ja siirtää puuttuvat tallenteet automaattisesti keskitettyyn järjestelmään yhteyden palautuessa. Tätä kutsutaan failover-tallennukseksi, ja sen etuna on katkeamaton videohistoria ilman jatkuvaa riippuvuutta verkkoyhteyden toimivuudesta (Axis Communications, 2021).

Reunatallennuksen rajoitteena on paikallisen tallennuskapasiteetin rajallisuus sekä hallinnan hajautuminen verrattuna puhtaasti NVR-pohjaiseen ratkaisuun. Lisäksi tallennusmedian, kuten microSD-korttien, kuluminen on huomioitava. Axis suosittelee valvontakäyttöön suunniteltujen, korkean kestävyyden surveillance-korttien käyttöä, joiden kirjoituskestävyys on merkittävästi parempi kuin tavallisilla kuluttajakorteilla (Axis Communications, 2021).

NAS-pohjainen tallennus

NAS-pohjaisessa tallennuksessa videodata tallennetaan erilliseen verkkoon liitettyyn tallennuslaitteeseen, joka tarjoaa jaettua tallennuskapasiteettia useille järjestelmän komponenteille. Axisin IP-Surveillance Design Guide -julkaisun mukaan NAS-ratkaisut soveltuvat erityisesti tilanteisiin, joissa tallennuskapasiteetin tarve on suuri tai tallenteita halutaan säilyttää pitkään arkistointitarkoituksiin (Axis Communications, 2007).

NAS-ratkaisun etuna on hyvä skaalautuvuus ja mahdollisuus hyödyntää RAID-tekniikoita sekä redundanssia. Toisaalta NAS lisää järjestelmän monimutkaisuutta ja asettaa vaatimuksia verkon suorituskyvylle, sillä tallennus ja mahdollinen arkistointi kuormittavat verkkoyhteyksiä erityisesti usean kameran järjestelmissä. Axisin mukaan pienissä ja keskisuurissa kohteissa NAS voi lisätä järjestelmän monimutkaisuutta ilman merkittävää operatiivista hyötyä verrattuna suoraan NVR-pohjaiseen tallennukseen (Axis Communications, 2007).

5 Kameravalvontaratkaisun valinta ja perustelut

5.1 Kameravalvontavalmistajien vertailu

Kameravalvontajärjestelmän valinta perustui sekä tekniseen vertailuun että asiakkaan käytännön tarpeisiin. Vertailuun otettiin kaksi valmistajaa: Ubiquiti UniFi ja TP-Link, koska molemmat tarjoavat lisenssimaksuttomia IP-kameravalvontaratkaisuja, jotka soveltuvat pieniin ja keskisuuriin kohteisiin.

Vertailun keskeiseksi lähtökohdaksi määriteltiin järjestelmän hallittavuus ei-teknisessä käyttöympäristössä. Järjestelmän käyttöliittymän selkeys, toimintalogiikan johdonmukaisuus sekä ylläpidon yksinkertaisuus korostuivat enemmän kuin yksittäiset tekniset ominaisuudet tai laitekohtaiset erot.

Toiseksi keskeiseksi vertailukriteeriksi nousi järjestelmän kokonaisarkkitehtuuri ja skaalautuvuus. Järjestelmän tuli mahdollistaa kameroiden ja tallennuskapasiteetin laajentaminen ilman, että hallintamalli tai käyttökokemus muuttuu olennaisesti. Lisäksi tapahtumapohjainen tallennus ja perusluonteiset kohteiden tunnistustoiminnot nähtiin hyödyllisinä lisäominaisuuksina, mutta eivät yksin ratkaisevina tekijöinä. Valmistajien välisiä eroja on koottu taulukkoon 2.

Ominaisuus	UniFi Protect	TP-Link VIGI
Tallennusmalli	Keskitetty NVR-pohjainen	Keskitetty NVR-pohjainen
Reunatallennus	Tuettu osassa kameroista microSD-kortilla täydentävä puskurina ja varmistuksena.	Reunatallennus mahdollinen microSD-kortilla tietyissä malleissa-
Käyttöliittymä	Yksi yhtenäinen hallintanäkymä verkko- ja kameralaitteille (UniFi Network / Protect)	Erillinen VIGI-hallinta. Verkkolaitteet eri järjestelmässä.
Lisenssimalli	Ei lisenssejä missään käyttötavassa. Toiminnot käytettävissä paikallisesti.	Ei lisenssejä NVR-pohjaisessa käytössä. Hallinta ja etäkäyttö nojaavat pilvipalveluun.

AI-ominaisuudet	Tapahtumapohjainen tallennus sekä henkilö- ja ajoneuvotunnistus tietyissä malleissa.	Vastaavat perus-AI-toiminnot kameramallin mukaan.
Skaalautuvuus	Skaalautuu hallitusti ilman muutoksia käyttölogiikkaan tai hallintamalliin.	Skaalautuva, mutta hallintaympäristö monimutkaistuu järjestelmän kasvaessa.

Taulukko 2. Unifi vs TP-Link – ominaisuuksien vertailu.

5.2 Kameravalvontalaitteiston valinnan perustelu

UniFi-järjestelmän valintaan vaikutti ratkaisevasti se, että yrityksellä oli jo ennestään käytössä UniFi-sarjan laitteita testikäytössä oppilaitoksen kautta. Demoasennusten perusteella järjestelmän hallintarajapinta, käyttölogiikka ja kuvanlaatu vastasivat hyvin sekä yrityksen että loppukäyttäjän odotuksia.

Käytännön testaus osoitti, että UniFi-järjestelmän vahvuus ei ole yksittäisissä teknisissä ominaisuuksissa, vaan kokonaisuuden hallittavuudessa. Verkko- ja kameralaitteet hallitaan samasta käyttöliittymästä, mikä vähentää ylläpidon kuormitusta ja pienentää virhekonfiguraation riskiä. Tämä on merkittävä etu ympäristössä, jossa järjestelmää ylläpitää rajallinen määrä henkilöitä ilman jatkuvaa teknistä tukea.

TP-Linkin VIGI-järjestelmä todettiin teknisesti toimivaksi ja ominaisuuksiltaan kilpailukykyiseksi vaihtoehdoksi. Sen hallintamalli on kuitenkin hajanaisempi, sillä verkko- ja kameraratkaisut eivät muodosta yhtä yhtenäistä kokonaisuutta. Tämä lisää järjestelmän konseptuaalista monimutkaisuutta ja kasvattaa ylläpidon vaatimuksia järjestelmän laajentuessa.

5.3 Kameravalvontaekosysteemien yhteensopivuus

UniFi-ekosysteemi muodostaa yhtenäisen ympäristön, jossa verkkolaitteet, valvontajärjestelmä ja hallinta-alusta toimivat saumattomasti keskenään. Tämä yhteensopivuus on erityisen tärkeää pienissä ja keskisuurissa asennuksissa, joissa hallinnan ja ylläpidon keskittäminen vähentää virheiden mahdollisuutta.

Ekosysteemin etuna on, että kaikki laitteet käyttävät samaa kontrolleria ja käyttöliittymäperiaatetta. Käyttäjän ei tarvitse siirtyä useisiin eri hallintasovelluksiin, vaan esimerkiksi

kytkimet, reititin ja kamerat näkyvät yhtenä kokonaisuutena. Tämä parantaa konfiguraation läpinäkyvyyttä ja nopeuttaa vianmääritystä.

Ekosysteeminen rakenne myös varmistaa, että ohjelmistopäivitykset ja turvallisuuskorjaukset julkaistaan samanaikaisesti ja testattuina toisiaan vasten. Tämä vähentää yhteensopivuusongelmia ja tekee kokonaisuudesta toimintavarman. Toisaalta suljetun ekosysteemin käyttö sitoo järjestelmän tiettyyn valmistajaan, mikä on huomioitava riskianalyysissä (ks. 5.5).

5.4 Kameravalvontaratkaisun kustannustarkastelu

Kokonaiskustannusten vertailussa UniFi erottui edukseen erityisesti lisenssimaksuttomuuden ansiosta. Järjestelmä ei edellytä kuukausi- tai vuosilisenssejä, vaan laitteiden hankintahinta kattaa ohjelmiston ja päivitysten käytön. Tämä alentaa ylläpitokustannuksia ja tekee kokonaiskustannusten ennakoinnista selkeämpää.

Kustannuksiin vaikuttavat lisäksi tallennuslevyjen ja verkkokomponenttien hinnat. Nämä muodostavat kertaluonteisen investoinnin, jonka suuruus riippuu tallennuskapasiteetin mitoituksesta ja kameroiden määrästä. Kilpaileviin ratkaisuihin, kuten pilvipohjaisiin tai lisenssipohjaisiin valvontajärjestelmiin verrattuna, kokonaisratkaisu on pitkällä aikavälillä kustannustehokas ja hallittavissa omassa infrastruktuurissa ilman ulkoisia palvelusopimuksia.

5.5 Kameravalvontaratkaisun rajoitukset ja riskit

Valittuun ratkaisuun liittyy tunnistettuja teknisiä ja toiminnallisia riskejä. Äänentallennus lisää tietosuojariskejä, minkä vuoksi järjestelmän käyttö edellyttää selkeitä käyttöoikeus- ja säilytyskäytäntöjä sekä lainsäädännön noudattamista.

Teknisinä rajoitteina tunnistettiin PoE-budjetti ja virransyötön mitoitus, jotka voivat vaikuttaa järjestelmän toimintavarmuuteen, mikäli niitä ei huomioida suunnitteluvaiheessa. Lisäksi valaistusolosuhteet vaikuttavat kuvanlaatuun erityisesti ulkokäytössä, mikä voi edellyttää täydentäviä valaistusratkaisuja.

Ekosysteemiriippuvuus on strateginen riski, mutta tässä toteutuksessa sen arvioitiin olevan hyväksyttävä, koska järjestelmän hallittavuus ja käyttövarmuus tuottavat enemmän hyötyä kuin avoimen järjestelmän tarjoama joustavuus.

5.6 Yhteenveto kameravalvontaratkaisusta

Järjestelmien vertailun, demovaiheen ja asiakkaan tarpeiden analyysin perusteella UniFi-pohjainen kameravalvontaratkaisu osoittautui kokonaistaloudellisesti ja toiminnallisesti

tarkoituksenmukaisimmaksi vaihtoehdoksi. Valinta perustui erityisesti järjestelmän yhtenäiseen hallintamalliin, helppokäyttöisyyteen ja ennakoitavaan kustannusrakenteeseen.

Vaikka TP-Linkin ratkaisu on teknisesti kilpailukykyinen, UniFi tarjoaa tässä kohteessa paremmin hallittavan ja käyttäjäystävällisemmän kokonaisuuden, joka tukee järjestelmän käyttöä ja laajentamista ilman merkittäviä rakenteellisia muutoksia.

6 Kameravalvontajärjestelmän toteutus ympäristössä

6.1 Kameravalvontaratkaisun lähtötilanne ja toteutusympäristö

Kameravalvontajärjestelmä toteutettiin yrityksen sisä- ja ulkotiloihin kaksikerroksiseen rakennukseen, jossa verkkolaitteet keskitettiin tekniseen tilaan. Toteutuksen tavoitteena oli parantaa asiakkaiden, henkilökunnan ja kiinteistön turvallisuutta sekä rakentaa ylläpidettävä ja selkeä verkkoinfrastruktuuri, joka tukee valittua kameravalvonta-alustaa.

Toteutusympäristö osoittautui teknisesti haastavaksi, koska rakennuksen sisäisestä kaapeloinnista ei ollut ajantasaista dokumentaatiota ja porttien nimeäminen oli puutteellista. Lisäksi osa verkkoyhteyksistä ei täyttänyt kaapeloinnille asetettuja vaatimuksia. Näistä syistä työn alkuvaiheessa painottuivat kaapeloinnin kartoitus, mittaukset ja dokumentointi, jotka loivat edellytykset luotettavalle verkko- ja kamerajärjestelmälle.

6.2 Kameravalvonnan demoympäristön tarkoitus ja toteutus

Ennen varsinaisen tuotantoympäristön käyttöönottoa järjestelmää testattiin erillisessä demoympäristössä. Demovaiheen tavoitteena oli varmistaa, että valittu kameravalvonta-alusta ja verkkorakenne toimivat suunnitellulla tavalla sekä mahdollistaa tilaajalle käytännön tutustuminen järjestelmään ennen lopullisia laitehankintoja. Lisäksi demoympäristö vähensi käyttöönottoon liittyviä riskejä ympäristössä, jossa kaapeloinnin kunto ja porttien toimivuus olivat alkuvaiheessa osin tuntemattomia.

Demoympäristö rakennettiin LAB-ammattikorkeakoulun lainalaitteistolla. Kokoonpanoon sisältyi reitittävä päätelaite (UDM Pro), IP-kameroita (G3 Flex ja G3 Bullet), kaksi langatonta tukiasemaa (U6 Long Range) sekä pienikokoisia PoE-kytkimiä. Vaikka laitteet eivät kaikilta osin vastanneet lopullista tuotantokokoonpanoa, ne mahdollistivat keskeisten toimintojen arvioinnin: kameroiden käyttöönoton, PoE-virransyötön, videovirtojen siirron, tallennuksen sekä käyttöliittymän ja etäkäytön testaamisen hallitussa ympäristössä.

Demovaiheessa toteutettiin valvontajärjestelmän perustoiminnallisuudet, kuten live-kuvan tarkastelu, tallenteiden muodostuminen ja yleinen toiminta. Samalla arvioitiin järjestelmän hallinnan keskittämistä, käyttöoikeuksien perusmallia sekä sitä, miten kameravalvonnan liikenne voidaan erottaa muusta verkkoliikenteestä loogisesti. Näin demoympäristö tuki sekä teknistä varmistusta että myöhempää arkkitehtuurisuunnittelua.

Tilaaja osallistui demovaiheen arviointiin ja sai kokemusta järjestelmän käyttöliittymästä ja päivittäisestä käytöstä. Havainnot liittyivät erityisesti käyttöliittymän selkeyteen, kuvanlaatuun sekä keskitetyn hallinnan etuihin verrattuna aiempiin ratkaisuihin. Demoympäristön

perusteella voitiin todentaa valitun kokonaisuuden soveltuvuus ja siirtyä tuotantoympäristön suunnitteluun ja toteutukseen varmuudella.

6.3 Kameravalvontaverkon rakenteen suunnittelu

Verkkorakenteen suunnittelun tavoitteena oli muodostaa loogisesti selkeä, turvallinen ja hallittava kokonaisuus, joka tukee IP-pohjaisen kameravalvontajärjestelmän vaatimuksia ilman, että muu yritysverkko kuormittuu tai altistuu tarpeettomille riskeille. Suunnittelussa painotettiin erityisesti liikenteen loogista eristämistä, keskitettyä hallittavuutta sekä mahdollisuutta laajentaa järjestelmää myöhemmin ilman merkittäviä rakenteellisia muutoksia.

Verkon ydin muodostuu yhdestä reitittävästä päätelaitteesta (UDM), joka toimii samanaikaisesti reitittimenä, palomuurina, VLAN-reitittäjänä sekä verkon hallintaympäristönä. Kaikki Layer 3 -toiminnot, kuten VLAN-verkkojen välinen reititys ja palomuurisäännöt, on keskitetty tähän laitteeseen. Erillistä fyysistä reitityskerrosratkaisua ei toteutettu, vaan arkkitehtuuri perustuu yhteen keskitettyyn L3-laitteeseen.

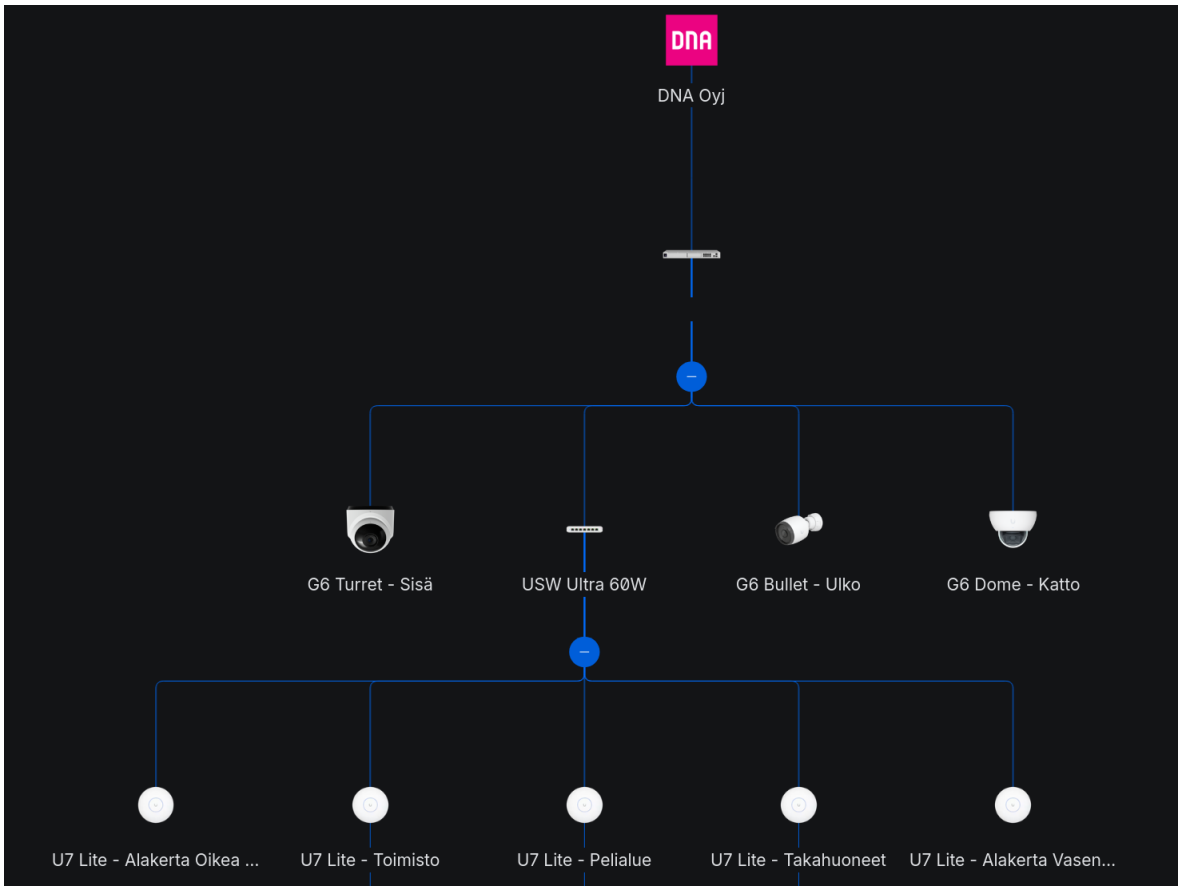
Fyysinen kytkentärakenne on tähtimallinen. Osa päätelaitteista, kuten kamerat, on liitetty suoraan reitittävään päätelaitteeseen, kun taas langattomat tukiasemat on liitetty erilliseen PoE-kytkimeen, joka toimii access-tason Layer 2 -kytkimenä. Näin ollen Layer 2 -toiminnot eivät muodosta omaa erillistä kytkentäkerrosta, vaan ne jakautuvat UDM:n sisäisten kytkentäporttien sekä erillisen access-kytkimen välille.

Kameravalvontajärjestelmälle määritettiin oma VLAN-segmentti, joka erottaa valvontaliikenteen käyttäjäverkoista ja vierasverkoista. Looginen segmentointi toteutettiin VLAN-tekniikalla, ei fyysisellä erillisverkolla. Näin kameraliikenne ei jaa samaa broadcast-domainia käyttäjäverkon kanssa, vaikka osa laitteista on fyysisesti samassa runkolaitteessa.

Langaton verkko on toteutettu erillisen kytkimen kautta liitetyillä tukiasemilla. Tukiasemien SSID-verkot on sidottu omiin VLAN-verkkoihinsa, jolloin käyttäjä-, vieras- ja mahdollinen IoT-liikenne voidaan erottaa toisistaan loogisesti. Kamerat on liitetty ensisijaisesti langallisesti, mikä varmistaa yhteyden vakauden sekä PoE-virransyötön.

Arkkitehtuuri on tarkoituksellisesti pidetty yksinkertaisena. Erillistä distribuutio- tai core-kerrosta ei ole, koska kohteen laitemäärä ja liikennemäärät eivät sitä edellytä. Keskitetty rakenne vähentää konfiguraation monimutkaisuutta ja helpottaa ylläpitoa.

Verkon yleiskaavio on esitetty kuviossa 3.



Kuvio 3. Verkon topologiakuva. Oma tuotanto.

6.4 Kameravalvonnan kaapeloinnin kartoitus, testaus ja dokumentointi

Kaapeloinnin kartoitus, testaus ja dokumentointi muodostivat keskeisen osan toteutusvaihetta, sillä olemassa olevan infrastruktuurin tila oli lähtötilanteessa suurelta osin tuntematon. Rakennuksen teknisessä tilassa sijaitsi laaja RJ45-liitäntäpaneeli, mutta porttien nimeäminen oli puutteellista eikä kaapelireittien todellisesta kulusta ollut käytettävissä ajantasaista dokumentaatiota. Tämä muodosti merkittävän riskin sekä verkon toimivuudelle, että kameravalvontajärjestelmän luotettavalle käyttöönotolle.

Kartoitus aloitettiin systemaattisella fyysisellä inventoinnilla. Jokainen teknisen tilan portti käytiin läpi ja yhteydet tunnistettiin vaiheittain kenttämittauksilla ja päätepisteiden paikantamisella. Löydetyt yhteydet nimettiin yhtenäisen nimeämiskäytännön mukaisesti, jossa porttitunnus, kerros ja päätepiste on yksiselitteisesti pääteltävissä. Fyysisen porttikohtaisen nimeämisen toteutusta havainnollistetaan kuvassa 3.

Kuva 3. RJ45-liitäntäpaneelin portin nimeäminen osana kaapeloinnin kartoitusta ja dokumentointia. Oma tuotanto.

Nimeämiskäytäntö mahdollistaa myöhemmän ylläpidon ja vianetsinnän ilman erillisiä lisäselvityksiä.

Kaapeloinnin tekninen kunto varmistettiin mittaamalla yhteydet ammattikäyttöön tarkoitetulla kaapelintestauslaitteella. Mittauksissa tarkasteltiin muun muassa johtimien jatkuvuutta, parikytkentöjä ja signaalin vaimennusta. Useat yhteydet eivät läpäisseet vaatimuksia, ja osassa kaapelivedoista havaittiin selkeitä virheitä, jotka ilmenivät epäonnistuneina mittaustuloksina. Nämä puutteet rajoittivat erityisesti PoE-virransyötön luotettavuutta ja estivät joidenkin reittien käyttämisen kriittisissä yhteyksissä.

Mittausvaiheessa havaittiin myös, että osa kaapeloinneista ei soveltunut jatkuvaan tai kuormitettuun käyttöön, kuten kameravalvonnan videoliikenteeseen. Erityisesti runkoyhteyksiksi suunnitelluilla reiteillä esiintyneet virheet edellyttivät vaihtoehtoisten kaapelireittien hyödyntämistä tai huomioimista myöhemmässä suunnittelussa. Joidenkin tilojen osalta todettiin, että toimivan ja vaatimukset täyttävän verkkoyhteyden toteuttaminen edellyttäisi rakennusteknisiä toimenpiteitä ja uudelleenkaapelointia.

Dokumentointi toteutettiin rinnakkain kartoituksen ja testauksen kanssa. Kaapelireitit, porttitunnukset, mittaustulokset ja havaitut puutteet kirjattiin järjestelmällisesti, ja alustavat kaaviot laadittiin vaiheittain täydentyvinä kokonaisuuksina. Dokumentaation tavoitteena oli tuottaa selkeä kokonaiskuva verkon fyysisestä rakenteesta ilman, että tieto jäisi yksittäisten mittausten tai havaintojen varaan.

Kaapeloinnin kartoitus ja dokumentointi muodostivat perustan koko verkkorakenteen jatkosuunnittelulle. Työvaihe mahdollisti toimivien ja luotettavien reittien tunnistamisen, riskialttiiden yhteyksien rajaamisen pois sekä tulevien kehitystoimenpiteiden perustellun suunnittelun. Samalla syntynyt dokumentaatio parantaa merkittävästi järjestelmän ylläpidettävyyttä ja vähentää virheiden todennäköisyyttä myöhemmissä muutoksissa.

6.5 Kameravalvonnan WLAN-suunnittelu ja mittaukset

Langattoman lähiverkon suunnittelun tavoitteena oli varmistaa riittävä peitto, kapasiteetti ja toimintavarmuus eri käyttäjäryhmille ilman, että langaton verkko muodostuu kameravalvontajärjestelmän kriittiseksi riippuvuudeksi. Kamerat liitettiin ensisijaisesti langallisesti, mutta WLAN:illa oli keskeinen rooli henkilöstön, asiakkaiden ja vieraiden verkkoyhteyksien tarjoamisessa.

WLAN-suunnittelu perustui kenttämittauksiin, joissa arvioitiin radiosignaalin leviämistä rakennuksen eri osissa ja kerrosten välillä. Mittauksissa hyödynnettiin useita eri tukiasemamalleja, joiden avulla voitiin tunnistaa tilojen vaimentavat rakenteet, mahdolliset häiriölähteet sekä optimaalinen tukiasemien sijoittelu. Vaikka mittauksissa käytetyt tukiasemat eivät kaikilta osin vastanneet lopullista laitevalintaa, ne tarjosivat riittävän pohjan peittoalueiden ja kapasiteettitarpeiden arviointiin.

Mittauksissa kiinnitettiin huomiota erityisesti seuraaviin tekijöihin:

- signaalin voimakkuuteen eri tiloissa
- signaalin läpäisyyn kerrosten välillä
- päällekkäisten peittoalueiden hallintaan
- kapasiteetin riittävyyteen käyttäjätiheyden kasvaessa.

Suunnittelun tuloksena tukiasemat sijoitettiin siten, että koko tila katetaan tasaisesti ilman tarpeetonta ylitystä tai katvealueita. Ratkaisussa huomioitiin myös se, että langaton verkko palvelee useita loogisia verkkoja samanaikaisesti VLAN- ja SSID-jakojen kautta. Näin sama fyysinen infrastruktuuri tukee useita käyttäjäryhmiä ilman, että niiden liikenne sekoittuu.

Langattoman verkon rooli rajattiin tietoisesti käyttäjä- ja asiakasliikenteeseen. Kameravalvontajärjestelmän kriittiset yhteydet eivät ole riippuvaisia WLAN-yhteyksistä, mikä parantaa koko järjestelmän toimintavarmuutta ja ennustettavuutta.

6.6 Kameravalvonnan WAN-yhteys ja etähallinta

WAN-yhteyden ja etähallinnan suunnittelun lähtökohtana oli varmistaa kameravalvontajärjestelmän jatkuva toiminta sekä mahdollistaa turvallinen ja hallittu etäkäyttö ilman, että

sisäverkkoon joudutaan avaamaan tarpeettomia yhteyksiä. Toteutusympäristössä kiinteää laajakaistayhteyttä ei ollut vielä käytettävissä, minkä vuoksi internet-yhteys toteutettiin mobiiliverkkoa hyödyntävällä SIM-korttipohjaisella reitittimellä.

Mobiiliyhteyden toimintavarmuus varmistettiin kartoittamalla rakennuksen sisätilojen signaalitasot. Reititin sijoitettiin paikkaan, jossa saavutettiin paras yhdistelmä signaalin voimakkuutta, yhteyden vakautta ja riittävää kapasiteettia. Signaalikartoituksen toteutusta havainnollistetaan kuviossa 4.

Kuvio 4 Rakennuksen sisätiloissa toteutettu mobiiliyhteyden signaalikartoitus. Oma tuotanto.

Reititysperiaatteet määriteltiin siten, että sisäverkko ja ulkoverkko ovat selkeästi erotettuja. Sisäverkoista sallitaan oletusarvoisesti vain tarvittava ulospäin suuntautuva liikenne, ja saapuva liikenne internetistä on estetty. Kameravalvontaverkolla ei ole suoraa pääsyä

internetiin, vaan mahdolliset ulkoiset yhteydet rajoittuvat järjestelmän hallinnan ja ohjelmistopäivitysten kannalta välttämättömiin toimintoihin. Tällä ratkaisulla pienennetään hyökkäyspintaa ja parannetaan koko järjestelmän tietoturvaa.

Etähallinta toteutettiin keskitetyn hallintamallin avulla, joka ei edellytä perinteisiä porttiohjauksia tai suoria yhteyksiä sisäverkkoon. Järjestelmän hallinta, valvonta ja vikatilanteiden analysointi ovat mahdollisia turvallisesti myös verkon ulkopuolelta. Tämä on erityisen tärkeää ympäristössä, jossa yhteys perustuu mobiiliverkkoon ja fyysinen pääsy kohteeseen ei ole aina mahdollista.

Tulevaisuuden tavoitetilana on siirtyminen kiinteään kuituyhteyteen, joka tarjoaa mobiiliyhteyttä paremman kapasiteetin, pienemmän viiveen ja ennustettavamman suorituskyvyn. Verkkorakenne ja reititysmalli on suunniteltu siten, että yhteystyypin vaihtaminen ei edellytä merkittäviä muutoksia sisäverkon rakenteeseen tai kameravalvontajärjestelmän toimintaan. Näin varmistetaan ratkaisun pitkäikäisyys ja joustavuus infrastruktuurin kehittyessä.

6.7 Kameravalvonnan VLAN- ja SSID-rakenne sekä eristysperiaatteet

Verkko jaettiin useisiin loogisiin VLAN-verkkoihin käyttötarkoituksen perusteella. Hallintaverkko on varattu verkkolaitteiden ja järjestelmän ylläpitoon, ja siihen on pääsy vain valtuutetuilla ylläpitolaitteilla. Henkilökunnan päätelaitteille määriteltiin oma VLAN, joka mahdollistaa pääsyn yrityksen sisäisiin palveluihin mutta ei suoraa yhteyttä kameraverkkoon. Kameravalvontajärjestelmälle määriteltiin erillinen VLAN, jossa sijaitsevat kaikki IP-kamerat sekä valvontaan liittyvät verkkolaitteet. Tämä verkko on tarkoituksella eristetty muista käyttäjäverkoista, ja sen liikenne on rajattu tallennus- ja hallintajärjestelmän suuntaan.

Vieraskäyttöä ja ulkopuolisia käyttäjiä varten toteutettiin oma vierasverkko, joka on täysin eristetty yrityksen sisäisistä verkoista. Vierasverkon liikenne ohjataan suoraan internetiin, eikä sillä ole pääsyä kameraverkkoon, hallintaverkkoon tai henkilökunnan verkkoon. Lisäksi ympäristössä on useita asiakas- ja vuokralaisverkkoja, jotka on toteutettu omilla VLANeilla. Näiden verkkojen välinen liikenne on estetty, jolloin kukin asiakas tai vuokralainen toimii omassa loogisessa verkossaan ilman mahdollisuutta päästä toisten verkkoihin tai yrityksen sisäisiin resursseihin.

Eristys toteutettiin sekä VLAN-tasolla että reitityspisteessä määritellyillä palomuurisäännöillä. VLAN:ien välinen liikenne on oletusarvoisesti estetty, ja poikkeukset on määritelty vain tarkasti rajattuihin käyttötapauksiin, kuten hallintaverkon pääsyyn kameroiden hallintaliittymiin ja tallennuspalvelimeen. Inter-VLAN-liikenteen rajoittaminen vähentää merkittävästi väärinkäytön ja virhetilanteiden vaikutuksia sekä parantaa koko verkon tietoturvaa.

Jokaiselle VLAN-verkkoon määriteltiin oma IP-osoiteavaruus ja sitä vastaava DHCP-pooli. Tämä selkeyttää verkon hallintaa ja mahdollistaa laitteiden yksiselitteisen tunnistamisen osoitealueen perusteella. Osoitteistus tukee myös vianetsintää ja dokumentointia, sillä verkon looginen rakenne on pääteltävissä suoraan IP-osoitteista ja VLAN-tunnisteista.

Langattoman verkon osalta SSID-rakenne sidottiin suoraan VLAN-verkkoihin. Henkilökunnan, vieraiden ja asiakkaiden langattomat verkot toimivat omilla SSID-tunnuksillaan, jotka ohjaavat liikenteen oikeaan VLANiin. Näin sama fyysinen tukiasemainfrastruktuuri palvelee useita käyttäjäryhmiä ilman, että niiden liikenne sekoittuu. Kamerat liitettiin ensisijaisesti langallisesti PoE:n kautta, mikä parantaa yhteyden luotettavuutta ja vähentää langattoman verkon kuormitusta.

Asiakkaiden ja vuokralaisten erottaminen toteutettiin sekä VLAN- että SSID-tasolla. Jokaiselle asiakkaalle tai vuokralaiselle määriteltiin oma looginen verkko, joka on eristetty muista asiakasverkoista ja yrityksen sisäisistä verkoista. Tämä ratkaisu tukee monitoimijaympäristön tietoturvaa ja selkeyttää verkon hallintaa.

Valmis VLAN- ja SSID-rakenne on havainnollistettu kuviossa 5.

Name	VLAN ID	Router	Subnet
Hallinta	1		10.0.0.0/24
Vieraat	20		10.20.0.0/24
Henkilökunta	10		10.10.0.0/24
Tulostin	40		10.40.0.0/24
Kamerat	30		10.30.0.0/24
Asiakas 1	60		192.168.10.0/24
Asiakas 2	70		192.168.20.0/24
Asiakas 3	80		192.168.30.0/24
Asiakas 4	90		192.168.40.0/24
Koti	2		192.168.2.0/24

Kuvio 5. VLAN-kartta ja looginen verkkorakenne toteutusympäristössä. Oma tuotanto.

6.8 Kameravalvontakameroiden sijoittelu ja asennusperiaatteet

Kameravalvontajärjestelmän sijoittelussa lähtökohtana oli tasapaino turvallisuuden, toiminnallisuuden ja yksityisyyden suojan välillä. Sijoittelua ohjasivat valvonnan tarkoitus, tilojen käyttötarkoitus sekä lainsäädännön asettamat rajoitteet. Kameroiden tehtävänä on tukea

tilojen ja omaisuuden suojaamista, ei kohdistaa jatkuvaa valvontaa yksittäisiin henkilöihin tai työpisteisiin.

Käytössä olevat kamerat edustavat eri laiteluokkia ja käyttötarkoituksia. Ulkoalueiden ja kulkureittien valvontaan hyödynnettiin säänkestäviä, pidemmän havaintoetäisyyden omaavia malleja, kun taas sisätiloissa käytettiin huomaamattomampia kameroita. Pienikokoisia ja joustavia malleja käytettiin tiloissa, joissa kameroiden näkyvyyden haluttiin olevan mahdollisimman hillitty. Kameramallien valinnassa huomioitiin kuvanlaatu, valonherkkyys, IR-valaistuksen ominaisuudet sekä yhteensopivuus järjestelmän muun infrastruktuurin kanssa.

Sijoitteluperiaatteissa keskeistä oli katvealueiden minimointi siten, että keskeiset kulkureitit ja sisäänkäynnit ovat valvonnan piirissä ilman, että kameroita kohdistetaan tarpeettomasti yksityisyyttä korostaviin alueisiin. Kameroita ei sijoitettu wc-, sosiaali- tai taukotiloihin, eikä niiden kuvakulma kohdistu työpisteisiin tavalla, joka mahdollistaisi työntekijöiden yksityiskohtaisen seurannan. Yöllistä kuvausta suunniteltaessa huomioitiin IR-valaistuksen kantama ja heijastukset, jotta kuvanlaatu säilyy riittävänä ilman ylivalotusta tai häiriöitä.

Rakennuksen eri kerrokset käsiteltiin sijoittelussa erillisinä kokonaisuuksina. Alakerran, yläkerran ja ulkoalueiden valvontatarpeet poikkeavat toisistaan sekä valaistusolosuhteiden että kulun luonteen osalta. Tästä syystä kameroiden määrää, tyyppiä ja sijoituskorkeutta tarkasteltiin kerroskohtaisesti. Ulkoalueilla huomioitiin lisäksi sääolosuhteet, valaisimet ja vuodenaikojen vaikutus kuvanlaatuun.

Kaapelireitit suunniteltiin siten, että asennus on siisti, turvallinen ja huollettava. Kaapelointi toteutettiin kiinteän verkon kautta, mikä parantaa yhteyden luotettavuutta ja mahdollistaa virransyötön PoE:n avulla. Kaapeleiden reitityksessä vältettiin näkyviä vetoja ja hyödynnettiin olemassa olevia kaapelireittejä aina kun se oli mahdollista. Tämä vähentää mekaanisia vaurioita ja helpottaa järjestelmän ylläpitoa.

Sähkösyötön osalta PoE-ratkaisu mahdollisti kameroiden keskitetyn virransyötön ilman erillisiä pistorasioita kamerapaikoissa. Tämä yksinkertaisti asennusta ja mahdollisti virransyötön hallinnan verkon kautta. PoE:n käyttö tukee myös järjestelmän vikasietoisuutta, sillä kameroiden tila ja virrankulutus ovat valvottavissa keskitetysti.

6.9 UniFi Protect –kameravalvonnan konfiguraation periaatteet

UniFi Protect toimii toteutetussa järjestelmässä kameravalvonnan keskitettynä hallinta- ja tallennusalustana. Sen avulla hallitaan kameroiden tallennusta, käyttöoikeuksia, hälytyksiä ja etäkäyttöä yhtenäisen käyttöliittymän kautta. Konfiguraation lähtökohtana oli muodostaa selkeä ja turvallinen kokonaisuus, jossa käyttäjien oikeudet, tallennusasetukset ja

hälytykset vastaavat sekä järjestelmän käyttötarkoitusta että lainsäädännön asettamia vaatimuksia.

Tallennusprofiilit määriteltiin kamerakohtaisesti siten, että ne vastaavat tilojen valvontatarpeita ja kuormitustasoa. Järjestelmä tukee sekä jatkuvaa tallennusta että tapahtumapohjaista tallennusta, jossa tallennus aktivoituu havaittujen tapahtumien perusteella. Profiilien avulla voitiin säätää muun muassa resoluutiota, kuvanopeutta ja tallennuksen aktiivisuutta eri vuorokaudenaikoina.

Älykkäät tunnistustoiminnot (Smart Detections) hyödynnettiin tukemaan tapahtumapohjaista valvontaa. Järjestelmä tunnistaa ennalta määriteltyjä kohdeluokkia, kuten henkilöitä ja ajoneuvoja, ilman yksilöivää biometristä tunnistamista. Tämä mahdollistaa olennaisten tapahtumien korostamisen ja vähentää tarpeettoman materiaalin kahlauksen määrää.

Hälytysasetukset suunniteltiin siten, että ne tukevat valvontaa ilman jatkuvaa hälytyskuormaa. Ilmoitukset perustuvat valittuihin tapahtumatyyppeihin ja toimitetaan vain niille käyttäjille, joilla on niihin tarve. Hälytysten tarkoituksena on tukea reagointia poikkeustilanteisiin, ei tuottaa jatkuvaa ilmoitusvirtaa normaalista toiminnasta.

Pääsynhallinta toteutettiin roolipohjaisena. Käyttäjille määriteltiin tehtävien mukaiset oikeudet, ja järjestelmään pääsy rajattiin vain niille henkilöille, joilla on siihen työtehtäviensä perusteella tarve. Etäkäyttö on mahdollista selainpohjaisen käyttöliittymän ja mobiilisovelluksen kautta keskitetyn hallintaratkaisun avulla ilman erillisiä porttiohjauksia.

6.10 Kameravalvonnan PoE-virrankulutus ja kapasiteetti

Power over Ethernet (PoE) -virransyötön mitoituksen tavoitteena oli varmistaa kameravalvontajärjestelmän häiriötön toiminta kaikissa käyttötilanteissa. PoE-kapasiteetin riittävyys korostuu erityisesti yöaikaan, jolloin IR-valaistus sekä kameran kuvanparannus- ja analytiikkatoiminnot voivat kasvattaa hetkellistä tehonkulutusta. Mikäli PoE-budjetti alittuu tai porttikohtainen tehoraja ylittyy, seurauksena voi olla kameran uudelleenkäynnistyminen tai katkokset tallennuksessa.

Järjestelmässä on käytössä kolme PoE-käyttöistä IP-kameraa: yksi UniFi Protect G6 Bullet, yksi G6 Turret ja yksi G6 Dome. Kameroiden maksimaalinen tehonkulutus määritettiin Ubiquitin julkaisemien teknisten tietojen perusteella: G6 Bullet 9,9 W, G6 Dome 9,25 W ja G6 Turret 12,5 W (Ubiquiti Inc., 2024a; Ubiquiti Inc., 2024b; Ubiquiti Inc., 2024c).

PoE-kokonaiskuormitus muodostettiin summaamalla kamerakohtaiset enimmäistehot (yhteensä 31,65 W). Tämän jälkeen kokonaiskulutukseen lisättiin 30 % mitoitusmarginaali, jolloin mitoituskuormaksi saatiin 41,145 W. Marginaali huomioi käytännön käyttötilanteita,

joissa kuormitus voi kasvaa samanaikaisesti esimerkiksi IR-valaistuksen aktivoituessa, kameran prosessoinnin lisääntyessä (esim. älytoiminnot ja kuvanparannus) sekä mahdollisten käynnistys- ja kytkentätilanteiden yhteydessä. Konservatiivinen mitoitus on perusteltu valvontajärjestelmissä, joissa virransyötön vakaus vaikuttaa suoraan järjestelmän luotettavuuteen.

Kamerat on liitetty suoraan UniFi Dream Machine Special Edition -laitteen PoE-portteihin. Valmistajan mukaan laitteen kokonais-PoE-budjetti on 180 W (Ubiquiti Inc., 2024d). Kun mitoituskuorma 41,145 W suhteutetaan kokonaisbudjettiin, järjestelmään jää PoE-kapasiteettia 138,855 W. PoE-budjetin laskenta on koottu taulukkoon, joka esitellään seuraavassa kuvassa 4, joka toimii myös samalla dokumentaationa nykyisestä kapasiteetista ja tukee myöhempää laajennus- ja muutossuunnittelua.

Kamera	Lukumäärä	Max tehonkulutus (W)	Kokonaisteho (W)
UniFi Protect G6 Bullet	1	9.9	9.9
UniFi Protect G6 Turret	1	12.5	12.5
UniFi Protect G6 Dome	1	9.25	9.25
Kokonaiskuormitus (max)			31.65
Mitoitusmarginaali 30%			41.145
PoE budjetti (W)			180
Jäljellä oleva kapasiteetti (W)			138.855

Kuva 4. PoE-budjetin laskenta IP-kameroille (maksimitehot ja 30 % mitoitusmarginaali). Oma tuotanto.

Laskennan perusteella voidaan todeta, että käytössä oleva PoE-kapasiteetti on selvästi riittävä nykyiselle kamerakokoonpanolle myös mitoitusmarginaali huomioiden. Lisäksi järjestelmään jää merkittävä kapasiteettivara, joka mahdollistaa uusien kameroiden tai muiden PoE-laitteiden liittämisen ilman tarvetta virransyöttöinfrastruktuurin muutoksille.

6.11 Kameravalvonnan tallennustilan mitoitus ja retentio

Kameravalvontajärjestelmän tallennustilan mitoitus on useista muuttujista riippuva kokonaisuus, jota ei voida määrittää yksiselitteisesti pelkän resoluution ja tallennuskapasiteetin perusteella. Tallennustilan kulutukseen vaikuttavat muun muassa videopakkausmenetelmä, bittinopeus, kuvataajuus (FPS), GOP-rakenne, kuvassa esiintyvä liike sekä valaistusolosuhteet. Erityisesti 4K-resoluutiolla bittivirran vaihtelu voi olla merkittävää, mikäli käytössä on muuttuva bittinopeus (VBR).

Järjestelmässä on käytössä kolme 4K-resoluutiolla tallentavaa IP-kameraa sekä noin 4 teratavun tallennuskapasiteetti. Tallennustilan mitoituksessa ei pyritty laskennallisesti tarkkaan ennusteeseen, vaan käytettiin käytännönläheistä ja vaiheittaista lähestymistapaa. Alkuvaiheessa määritettiin tarkoituksenmukaiset perusasetukset videopakkaukselle,

bittinopeudelle ja kuvataajuudelle siten, että kuvanlaatu vastaa kohteen turvallisuusvaatimuksia ilman tarpeetonta tallennustilan kuormitusta.

Tallennusratkaisu perustuu jatkuvaan tallennukseen sekä automaattiseen tilanhallintaan, jossa vanhimmat tallenteet poistuvat kapasiteetin täyttyessä. Tällainen kiertävä tallennusperiaate (rolling retention) on tyypillinen yritysympäristöissä, joissa tavoitteena ei ole pitkäaikainen arkistointi vaan tapahtumien jälkikäteinen tarkastelu rajatulta aikaväliltä.

Teoreettista arviota täydennettiin järjestelmän todelliseen käyttöön perustuvalla havainnolla. Tarkasteluhetkellä 2.1.2026 tallennusjärjestelmä sisälsi videomateriaalia ajankohdasta 18.12.2025 alkaen, mikä tarkoittaa noin 15 vuorokauden yhtäjaksoista säilytysaikaa kolmen 4K-kameran kokoonpanolla. Havainto osoittaa, että asetettu bittinopeus- ja pakkauskonfiguraatio tuottaa käytännössä riittävän retentioajan järjestelmän käyttötarkoitukseen nähden.

Tallennustilan mitoitusta ei siten pidetty staattisena kertaluonteisena laskelmana, vaan sitä käsiteltiin dynaamisena parametrina. Järjestelmän käyttöä seurataan, ja tallennusasetuksia voidaan tarvittaessa säätää esimerkiksi pienentämällä kuvataajuutta, optimoimalla bittinopeutta tai lisäämällä tallennuskapasiteettia. Tällainen iteratiivinen optimointi on suositeltava käytäntö, koska todellinen tallennustarve määräytyy vasta käyttöympäristössä.

Säilytysaika on riittävä järjestelmän käyttötarkoitukseen ja tukee tietosuojaperiaatetta, jonka mukaan henkilötietoja ei säilytetä pidempään kuin on tarpeen. Mikäli säilytysaikaa halutaan pidentää, se voidaan toteuttaa joko lisäämällä tallennuskapasiteettia tai muuttamalla tallennusparametreja.

7 Työvaiheet ja mittaustulokset

7.1 Käsitteiden pohjustus

Tässä alaluvussa kuvataan kaapelointimittausten kannalta keskeiset käsitteet, joita hyödynnetään mittaustulosten esittämisessä ja tulkinnassa seuraavissa alaluvuissa.

Attenuation (Insertion Loss)

Attenuationilla eli insertion lossilla tarkoitetaan signaalin vaimenemista kaapelointilinkissä siirryttäessä lähettävästä päästä vastaanottavaan päähän. Ilmiö johtuu kaapelin sähköisistä ominaisuuksista ja aiheuttaa signaalin heikkenemistä linkin pituuden ja siirtotaajuuden kasvaessa. Insertion loss ilmoitetaan desibeleinä (dB) ja kuvaa signaalin tehohäviötä siirtotiellä. (Fluke Networks 2025.)

NEXT (Near-End Crosstalk)

NEXT (Near-End Crosstalk) kuvaa häiriötä, jossa yhden johtoparin signaali kytkeytyy sähkömagneettisesti viereiseen pariin kaapelointilinkin lähettävässä päässä. Ilmiö syntyy johtimien välisestä kytkeytymisestä ja korostuu erityisesti, jos parien kierre purkautuu liitoskohdissa. NEXT ilmaistaan desibeleinä (dB), ja suurempi arvo tarkoittaa vähäisempää häiriötä. (Fluke Networks 2025.)

Power Sum NEXT (PS NEXT)

Power Sum NEXT (PS NEXT) kuvaa useiden johtoparien yhteenlaskettua lähiläppäyshäiriötä yksittäiseen johtopariin. PS NEXT ei ole suoraan mitattu suure, vaan laskennallinen arvo, joka muodostetaan yksittäisten NEXT-mittausten perusteella. Suure on erityisen merkityksellinen neljän parin samanaikaista tiedonsiirtoa hyödyntävissä järjestelmissä. (Fluke Networks 2025.)

Return Loss

Return loss (RL) kuvaa lähetetyn ja heijastuneen signaalitehon suhdetta kaapelointilinkissä impedanssiepäsovitusten seurauksena. Impedanssiepäjatkuvuudet aiheuttavat osan signaalienergiasta heijastumaan takaisin lähettävään päähän. Return loss ilmoitetaan desibeleinä (dB), ja suurempi arvo tarkoittaa parempaa impedanssisovitusta sekä vähäisempää heijastunutta energiaa. (Fluke Networks 2025.)

Attenuation to Crosstalk Ratio Near-End (ACR-N)

ACR-N (Attenuation to Crosstalk Ratio Near-End) kuvaa vaimennuksen (insertion loss) ja lähiläppäyshäiriön (NEXT) välistä suhdetta kaapelointilinkin lähettävässä päässä. Suure

määritellään taajuuskohtaisesti vähentämällä vaimennus mitatusta NEXT-arvosta (ACR-N = NEXT − IL). ACR-N ilmaisee signaalin ja häiriön välisen häiriövaran, ja suurempi arvo tarkoittaa parempaa siirtokykyä kyseisellä taajuudella. (Fluke Networks 2025.)

ACR-F (Attenuation to Crosstalk Ratio Far-End)

ACR-F (Attenuation to Crosstalk Ratio Far-End) kuvaa vaimennuksen ja kaukoläppäyshäiriön (FEXT) välistä suhdetta kaapelointilinkin vastaanottavassa päässä. Suure määritellään vähentämällä linkin vaimennus mitatusta FEXT-arvosta, jolloin saadaan niin sanottu ACR-F (aiemmin ELFEXT). ACR-F ilmaisee vastaanottopään häiriövaran ja täydentää ACR-N-tarkastelua linkin kokonaislaadun arvioinnissa. Suurempi arvo tarkoittaa parempaa siirtokykyä. (Fluke Networks 2025.)

7.2 Projektiin liittyvä aikataulu

Projekti eteni vaiheittain ja osittain iteratiivisesti, mikä on tyypillistä käytännönläheisissä tietojärjestelmä- ja infrastruktuurihankkeissa. Työ käynnistyi ennakkosuunnittelulla ennen varsinaista kohdekäyntiä, ja jatkui kesän aikana aina järjestelmän käyttöönottoon ja testaukseen saakka.

Suunnitteluvaiheessa muodostettiin alustava käsitys järjestelmän vaatimuksista ja mahdollisista toteutusvaihtoehdoista. Tässä vaiheessa hyödynnettiin aiempaa tietoa IP-kameravalvontajärjestelmistä sekä toimeksiantajan esittämiä lähtötietoja. Varsinainen kohdekäynti tarkensi käsitystä ympäristöstä, kaapeloinnista ja olemassa olevasta verkkoinfrastruktuurista, minkä jälkeen suunnitelmaa täsmennettiin vastaamaan todellisia olosuhteita.

Demovaihe toteutettiin erillisessä testiverkossa, jossa järjestelmää kokeiltiin UniFi-laitteilla ennen lopullisten tuotantolaitteiden tilaamista. Demoympäristössä testattiin muun muassa verkon segmentointia, kameravalvontajärjestelmän toimintaa sekä keskitettyä hallintaa. Samalla dokumentoitiin verkon porttikytkennät ja kartoitettiin sopivimmat liityntäpisteet tuotantolaitteille. Demovaihe toimi tärkeänä riskienhallintakeinona ennen varsinaista käyttöönottoa.

Dokumentointia tehtiin koko projektin ajan rinnakkain muiden työvaiheiden kanssa. Dokumentaatio kattoi muun muassa verkkorakenteen, VLAN-jaot, porttikytkennät sekä järjestelmän yleisen rakenteen. Tämä helpotti myöhempää käyttöönottoa, testausvaihetta ja raportointia.

Varsinainen toteutusvaihe käynnistyi, kun lopulliset laitteet oli tilattu ja toimitettu. Tällöin demolaitteet korvattiin tuotantokäyttöön tarkoitetuilla laitteilla ja järjestelmä otettiin käyttöön suunnitelman mukaisesti. Toteutuksen jälkeen järjestelmälle suoritettiin testaus, jossa

varmistettiin kameroiden toiminta, tallennus, verkon eristys sekä etähallinnan luotettavuus. Testausvaiheen jälkeen järjestelmä jäi tuotantokäyttöön.

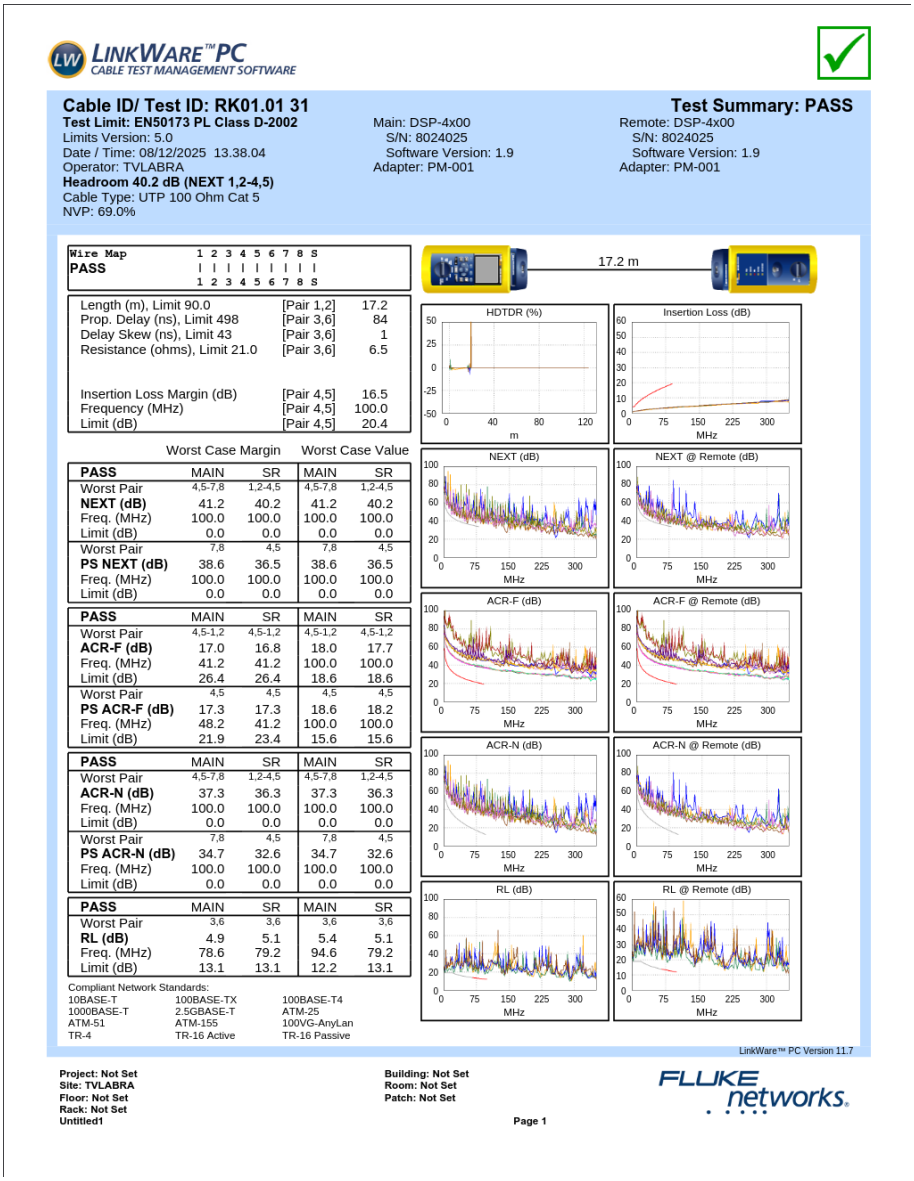
7.3 Kaapeloinnin testaus ja tulkinta Fluke DSP-4300 –analysaattorilla

Kameravalvontajärjestelmän kaapeloinnin toimivuus ja vaatimustenmukaisuus varmistettiin mittaamalla asennetut kuparikaapelilinkit Fluke DSP-4300 -kaapelianalysaattorilla. Mittaukset suoritettiin pysyvän linkin (permanent link) testiprofiililla EN 50173 Class D -raja-arvojen mukaisesti.

Fluke DSP-4300 -analysaattorin testaus perustuu laitteessa valittuun standardiprofiiliin, jonka raja-arvot pohjautuvat EN 50173 -luokituksen sähköisiin suorituskykyvaatimuksiin. Varsinainen mittausmenetelmä ja hyväksyntälogiikka perustuvat testauslaitteen käyttämään standardiprofiiliin, eivät suoraan EN 50173 -rakennestandardin soveltamiseen.

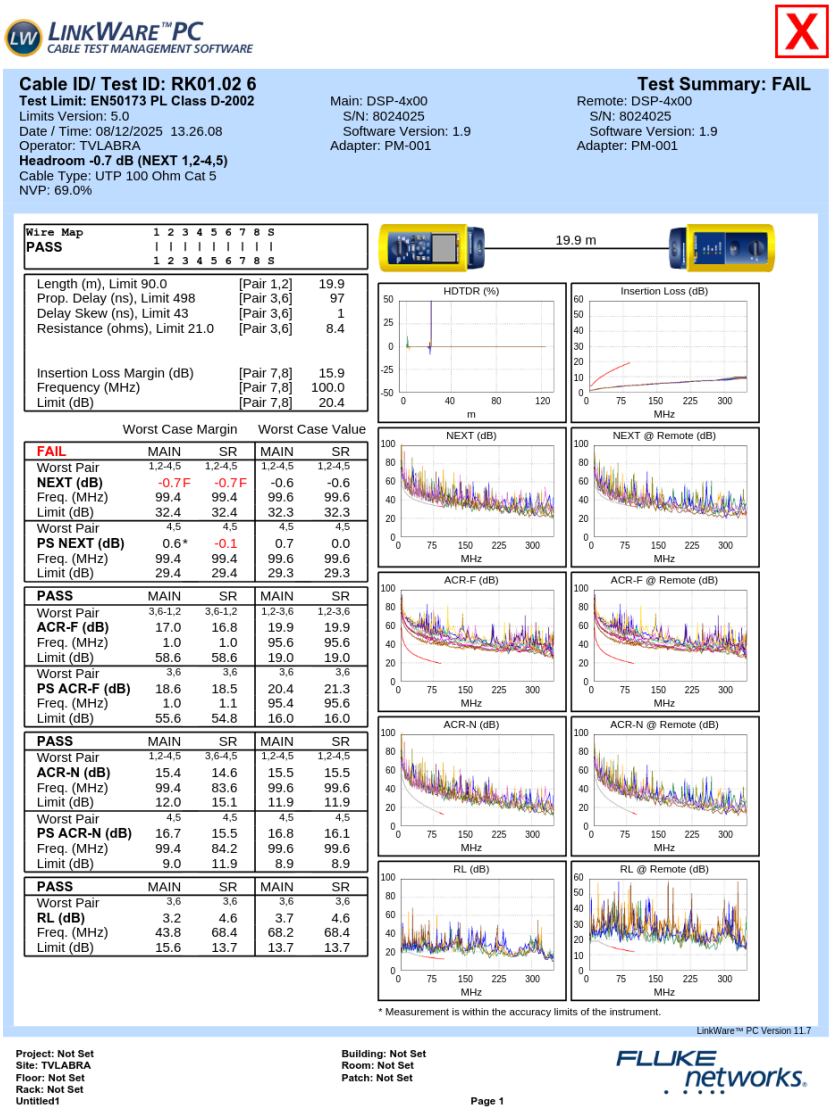
TIA-568-C-standardia hyödynnetään työssä ainoastaan terminologian ja teknisten periaatteiden rinnakkaisena viitekehyksenä, ei varsinaisena testauksen hyväksymisperusteena.

Mittausmenetelmä kattoi kaikki EN 50173 -standardissa määritellyt keskeiset sähköiset ominaisuudet, mukaan lukien johdotuksen eheyden, signaalin vaimennuksen, etenemisviiveet sekä parien väliseen häiriösuojaukseen liittyvät parametrit. Testausten tulkinta suoritettiin LinkWare PC -ohjelmistolla, ja jokaisesta mitatusta linkistä tallennettiin yksityiskohtainen PASS/FAIL-mittausraportti. Osiossa esitetään yksi edustava standardinmukainen PASS-raportti sekä yksi rajatapausta kuvaava FAIL-raportti, jotka havainnollistavat mittaustulosten vaihtelua käytännön kohteessa (kuvat 5 ja 6).



Kuva 5. Fluke DSP-4300 -mittausraportti: EN 50173 Class D -vaatimukset täyttävä pysyvä linkki (PASS). Oma tuotanto.

Mittausraportti osoittaa selkeät marginaalit kaikissa keskeisissä parametreissa, kuten NEXT-, insertion loss- ja return loss -arvoissa. Tulos edustaa kohteen standardinmukaista ja teknisesti hyvälaatuista kaapelointilinkkiä, joka soveltuu IP-pohjaiseen videoliikenteeseen ja PoE-virransyöttöön.



Kuva 6. Fluke DSP-4300 -mittausraportti: rajatapausta edustava linkki, jossa NEXT-alitus johti FAIL-luokitukseen. Oma tuotanto.

Mittausraportissa havaitaan NEXT-parametrin alitus hyvin pienellä marginaalilla (headroom −0,7 dB) korkeilla taajuuksilla, minkä seurauksena linkki luokiteltiin FAIL-tilaan. Wiremap ja muut keskeiset parametrit täyttävät kuitenkin vaatimukset. Tapaus havainnollistaa mittaustulosten tulkinnan merkitystä erityisesti lyhyissä kaapelointilinkeissä, joissa yksittäinen rajatapaus ei välttämättä johda välittömiin käytännön toimintahäiriöihin.

Mittausten yhteydessä testattiin yhteensä 28 kuparikaapelilinkkiä, joista valtaosa täytti EN 50173 Class D -vaatimukset kaikilta osin. Osa linkeistä luokiteltiin mittausraporteissa FAIL-tilaan yksittäisten mittausparametrien osalta. Hylkäykset liittyivät pääosin rajatapausarvoihin korkeilla taajuuksilla.

Wiremap-testit osoittivat, että lähes kaikissa tarkastelluissa linkeissä johdotusjärjestykset olivat oikein. Linkkien pituudet vaihtelivat noin 8–40 metrin välillä, mikä on selvästi alle EN 50173 -standardin salliman 90 metrin enimmäispituuden pysyvälle linkille. Lyhyet kaapelointimatkat näkyivät myös pieninä etenemisviiveinä ja vähäisinä viive-eroina (delay skew), jotka jäivät lähes kaikissa tapauksissa selvästi alle sallittujen raja-arvojen.

Insertion loss -mittaukset osoittivat, että signaalin vaimennus pysyi kaikilla mitatuilla taajuuksilla standardin sallimissa rajoissa, ja marginaalit olivat tyypillisesti yli 15 dB. Tämä on hyvä tulos kyseiselle kaapeliluokalle ja lyhyille linkkipituuksille. Tulokset osoittavat, että signaalin taso säilyy riittävänä koko linkin matkalla eikä vaimennus muodostu rajoittavaksi tekijäksi IP-pohjaisen videoliikenteen siirrossa.

NEXT- ja PSNEXT-mittauksissa havaittiin yksittäisiä rajatapauksia, joissa lähiparin ylikuuluminen alitti EN 50173 -standardin raja-arvon hyvin pienellä marginaalilla. Näiden ylitysten seurauksena osa linkeistä luokiteltiin mittausraporteissa FAIL-tilaan. Poikkeamat ilmenivät korkeilla taajuuksilla ja hyvin pienillä headroom-arvoilla (noin −0,1…−0,7 dB), mikä viittaa paikallisiin liitinhäiriöihin tai parien kierretiheyden heikkenemiseen liitoskohdissa.

Käytännön testauksessa kyseiset rajatapaukset eivät aiheuttaneet jatkuvia tai toistuvia häiriöitä kamerajärjestelmän normaalikäytössä kaikissa porteissa. Yksittäisiä yhteys- ja PoE-ongelmia havaittiin kuitenkin nimenomaan niissä linkeissä, joissa mittaustulokset jäivät lähelle raja-arvoja. Mittaustulokset eivät siten yksin selitä kaikkia havaittuja häiriöitä, mutta ne korreloivat heikompien porttien kanssa.

Return loss -mittaukset pysyivät pääosin hyväksytyissä rajoissa, mutta osassa linkeistä mitattiin pieniä marginaaleja. Tämä viittaa lieviin impedanssiepäjatkuvuuksiin, jotka ovat tyypillisiä erityisesti vanhemmissa Cat 5 -asennuksissa ja liittyvät useimmiten liittimien asennustapaan tai kaapeloinnin ikääntymiseen.

Kokonaisuutena kaapelointimittaukset osoittivat, että suurin osa linkeistä täytti vaatimukset, mutta yksittäisiä rajatapauksia ja selkeitä virheitä esiintyi. Mittaustulokset muodostivat perustan käytännön vianmääritykselle ja verkon porttien systemaattiselle kartoitukselle, joita käsitellään seuraavassa alaluvussa.

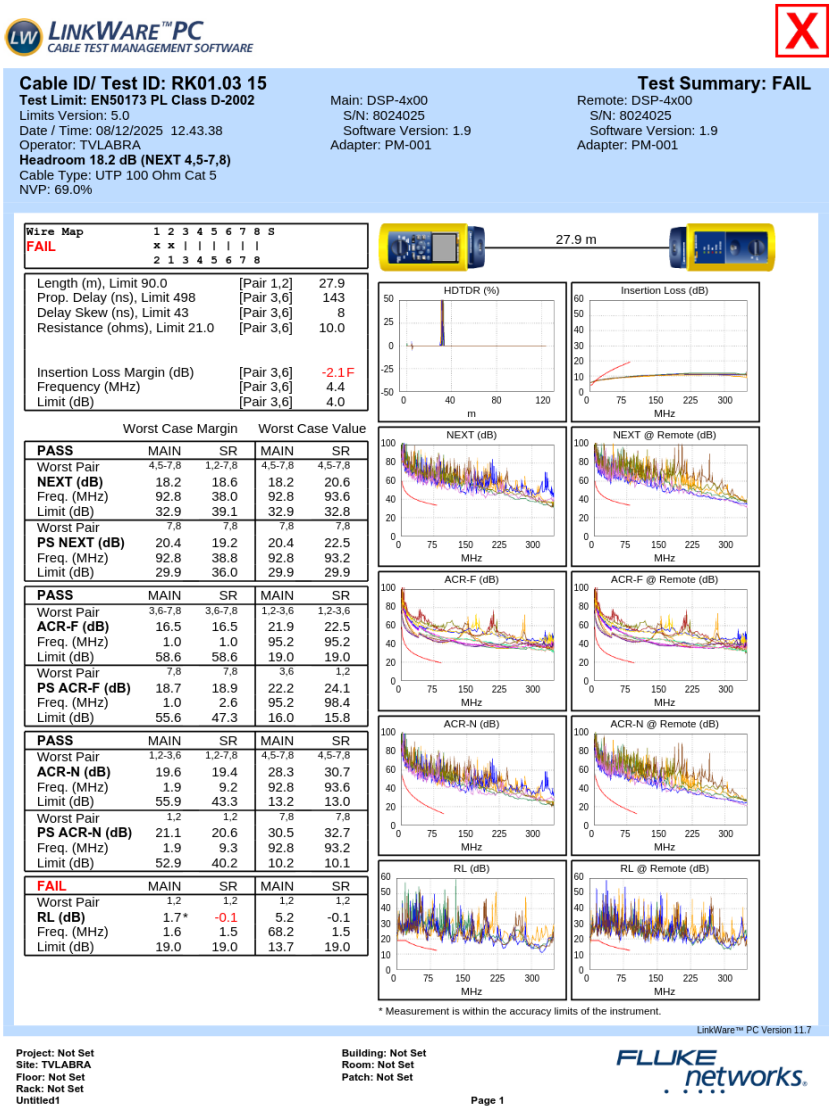
7.4 Havaitut viat, vianmääritys, ratkaisut sekä verkkoporttien dokumentointi

Kaapelointimittausten ja käytännön testauksen yhteydessä havaittiin useita verkon toimintaan vaikuttavia puutteita, jotka olivat tyypillisiä vanhemmalle ja puutteellisesti dokumentoidulle lähiverkkoasennukselle. Havaitut ongelmat liittyivät pääosin yksittäisiin heikkolaatuisiin portteihin, katkenneisiin tai virheellisesti päätettyihin johdinpareihin sekä epäselvään

porttien nimeämiseen ja dokumentointiin. Havainnot tukivat aiemmissa mittauksissa esiin nousseita rajatapauksia, joissa kaapeloinnin sähköiset ominaisuudet jäivät lähelle EN 50173 Class D -standardin raja-arvoja. Mittaustulosten ja käytännön oireiden välinen yhteys vahvisti käsitystä siitä, että havaitut häiriöt johtuivat ensisijaisesti passiivisen kaapelointi-infrastruktuurin ominaisuuksista eivätkä valitusta verkkoarkkitehtuurista tai aktiivilaitteiden kapasiteetista. Näin ollen ongelmien syy voitiin rajata fyysiseen siirtotiehen eikä järjestelmän suunnitteluperiaatteisiin.

Fluke DSP-4300 -mittausten perusteella osa linkeistä ei täyttänyt EN 50173 Class D -vaatimuksia kaikilta osin. Yleisimmät hylkäyssyyt liittyivät palautusvaimennukseen (return loss) sekä NEXT- ja PSNEXT-arvoihin, mikä viittaa erityisesti pääteltyjen liittimien laatuongelmiin.

Joissakin tapauksissa wiremap-testi paljasti selkeitä johdinparien katkoksia tai virheellisiä kytkentöjä, minkä seurauksena PoE-syöttö ei käynnistynyt tai verkkoyhteys ei muodostunut lainkaan. Tällainen tilanne on esitetty kuvassa 7, jossa mittaustulos hylättiin wiremap-virheen vuoksi. Näissä tapauksissa kameralaitteiden käyttöönotto epäonnistui kokonaan tai yhteys osoittautui epävakaaksi.



Kuva 7. Fluke DSP-4300 -mittausraportti: wiremap-testissä havaittu johdinparien virheellinen kytkentä, joka johti FAIL-luokitukseen. Oma tuotanto.

Vianmääritys toteutettiin systemaattisesti vertailemalla laitteiden toimintaa eri porteissa. Testauksessa laitteita siirrettiin portista toiseen ja seurattiin, siirtyikö vika portin mukana vai jäikö se tiettyyn päätelaitteeseen. Tämän avulla pystyttiin erottamaan toisistaan kaapelointiin liittyvät viat ja yksittäiset laiteviat. Esimerkiksi testikäytössä ollut kamera todettiin toimivaksi vaihdettaessa se toiseen porttiin, mikä viittasi ensisijaisesti kaapelointiongelmaan. Vastaavasti yksi kamera osoittautui vialliseksi, kun se oireili samalla tavalla useissa eri porteissa.

Heikkolaatuiset tai mittausten perusteella epäluotettaviksi todetut portit jätettiin pois käytöstä ja dokumentointiin, ja kamerat kytkettiin mitattuihin ja luotettaviksi todettuihin portteihin

verkkokaapin läheisyydessä. Mikäli yksittäinen linkki osoittautui toistuvasti ongelmalliseksi, sitä ei käytetty tuotantoympäristössä.

Teknisten kaapelointiongelmien lisäksi merkittävä haaste liittyi verkon aiempaan dokumentointiin. Verkkokaapissa oli useita kymmeniä RJ45-portteja, joiden alkuperäinen nimeäminen oli epäselvää tai puuttui kokonaan. Tämän vuoksi verkkoporttien kartoitus jouduttiin aloittamaan käytännössä alusta. Jokainen toimiva portti paikannettiin, testattiin ja nimettiin yhdenmukaisella tunnistejärjestelmällä, jossa portin tunnus ilmaisee rakennuksen, kerroksen ja seinärasian porttinumerot (esimerkiksi RK01.01.17–18). Sama tunniste merkittiin sekä verkkokaappiin että seinärasioihin, mikä parantaa jatkossa vianetsinnän ja muutostöiden hallittavuutta.

Porttikartoituksen yhteydessä laadittiin porttitaulukot, joihin dokumentoitiin porttien sijainti, käyttötarkoitus sekä niihin liitetyt laitteet. Dokumentointi tehtiin vaiheittain ja sitä täydennettiin projektin edetessä. Lopullinen dokumenttipaketti sisältää porttitaulukot, kaapelointimerkinnät sekä Fluke DSP-4300 -mittausraportit, ja se luovutettiin toimeksiantajalle osana projektin päätöstä. Dokumentoidun kokonaisuuden ansiosta verkon rakenne on jatkossa ymmärrettävä ja ylläpidettävä myös ilman alkuperäisten toteuttajien läsnäoloa.

Edellä kuvattujen toimenpiteiden jälkeen verkon toiminta stabiloitui, eikä tuotantokäytössä havaittu toistuvia yhteyskatkoksia tai PoE-syötön häiriöitä mitattuihin ja hyväksyttyihin portteihin kytketyissä kameroissa. Kaapelointiin ja verkkoportteihin liittyvät havainnot osoittivat, että kameravalvontajärjestelmän toimivuus ei ole riippuvainen pelkästään aktiivilaitteista, vaan myös passiivisen infrastruktuurin kunto ja dokumentointi ovat keskeisiä tekijöitä. Huolellisella mittaamisella, systemaattisella vianmäärityksellä ja selkeällä dokumentoinnilla pystyttiin varmistamaan kameravalvontajärjestelmän luotettava toiminta olemassa olevassa ympäristössä.

8 Kamerajärjestelmän toimivuus ja arviointi

8.1 Järjestelmän toimivuus ja käytännön havainnot

Kameravalvontajärjestelmä on toiminut suunnitellulla tavalla käyttöönoton jälkeen ja täyttänyt sille asetetut toiminnalliset ja tekniset tavoitteet. Kamerakuvat ovat olleet jatkuvasti saatavilla sekä paikallisesti että etäyhteyden kautta ilman merkittäviä katkoksia, mikä osoittaa järjestelmän perustoiminnallisuuden olevan vakaa.

Verkkotason toimivuus on ollut luotettavaa: kamerat ovat pysyneet jatkuvasti verkossa, PoE-virransyöttö on ollut vakaa eikä kameroiden odottamattomia uudelleenkäynnistymisiä ole havaittu. Tämä viittaa siihen, että sekä aktiivilaitteiden kapasiteetti että passiivinen kaapelointi ovat riittäviä järjestelmän kuormitukseen nähden. IP-pohjainen toteutus, VLAN-segmentointi ja keskitetty hallinta ovat tukeneet järjestelmän hallittavuutta ja eriyttäneet valvontaliikenteen muusta verkosta.

Tallennus on toiminut asetettujen tallennusprofiilien mukaisesti, ja vanhimmat tallenteet ovat poistuneet automaattisesti tallennustilan täyttyessä. Seurantajakson perusteella tallennusretentio vastaa mitoitusvaiheessa tehtyjä arvioita, eikä tallennuksessa ole havaittu keskeytyksiä. Tallenteiden selaaminen ja haku ovat olleet sujuvia sekä työasema- että mobiilikäytössä.

Kamerakuvien laatu on ollut käyttötarkoitukseen nähden hyvä sekä päivä- että yöolosuhteissa. IR-valaistus on ollut riittävä sisätiloissa ja katetuilla ulkoalueilla, eikä merkittäviä katvealueita ole havaittu. Kameroiden sijoittelu tukee valvonnan tarkoitusta ilman tarpeetonta puuttumista yksityisyyteen.

Kokonaisuutena järjestelmän toimivuutta voidaan pitää käyttötarkoitukseen nähden hyvänä. Kriittiset sisäiset toiminnot, kuten videon tallennus, paikallinen verkkoyhteys ja PoE-virransyöttö, eivät ole keskeytyneet käyttöönoton jälkeen. Etäyhteyksissä on havaittu satunnaisia katkoksia käytössä olleen SIM-pohjaisen WAN-yhteyden vuoksi, mutta nämä eivät ole vaikuttaneet videon tallentumiseen edge storage -ratkaisun ansiosta. Järjestelmä on jatkanut tallennusta normaalisti paikallisessa verkossa myös internet-yhteyden ollessa poikki. Suunniteltu siirtyminen kiinteään kuituyhteyteen parantaa jatkossa etäkäytön vakautta.

8.2 Havaitut haasteet ja luotettavuuden arviointi

Kameravalvontajärjestelmän käyttöönoton yhteydessä havaitut haasteet liittyivät pääosin olemassa olevaan passiiviseen infrastruktuuriin ja puutteelliseen porttidokumentointiin.

Kaapelointivirheet, rajatapaukset mittaustuloksissa sekä epäselvä porttien nimeäminen vastasivat aiemmissa mittauksissa ja vianmäärityksessä esiin nousseita havaintoja. Haasteet eivät kohdistuneet valittuun verkkoarkkitehtuuriin tai aktiivilaitteiden kapasiteettiin, vaan fyysiseen siirtotiehen ja ympäristön lähtötilanteeseen.

Luotettavuuden näkökulmasta järjestelmä on osoittautunut käyttötarkoitukseen nähden vakaaksi. Kamerat ovat pysyneet jatkuvasti yhteydessä paikallisverkkoon, PoE-virransyöttö on ollut riittävä ja videon tallennus on toiminut keskeytyksettä. Etäyhteyksissä havaitut satunnaiset katkokset johtuivat käytössä olleesta SIM-pohjaisesta WAN-yhteydestä, eivätkä ne vaikuttaneet paikalliseen tallennukseen edge storage -ratkaisun ansiosta. Järjestelmän kokonaisluotettavuutta voidaan siten pitää hyvänä, kun tarkastelu rajataan sen kriittisiin sisäisiin toimintoihin.

Luotettavuutta vahvistaa se, että keskeiset riskitekijät tunnistettiin ja käsiteltiin jo projektin aikana mittausten, vianmäärityksen ja dokumentoinnin avulla. Valittu verkkorakenne, segmentointi ja dokumentointikäytännöt tukevat järjestelmän ennakoitavaa toimintaa sekä mahdollistavat hallitun laajentamisen ja ylläpidon myös tulevaisuudessa.

8.3 Oppimiskokemukset

Opinnäytetyö tarjosi kokonaisvaltaisen oppimisprosessin, jossa yhdistyivät tekninen suunnittelu, käytännön toteutus ja järjestelmän arviointi todellisessa käyttöympäristössä. Työ osoitti, että toimivan kameravalvontajärjestelmän toteuttaminen ei ole pelkästään laitteiden asentamista, vaan edellyttää kokonaisvaltaista ymmärrystä verkkoarkkitehtuurista, tietoturvasta, lainsäädännöstä sekä järjestelmällisestä dokumentoinnista.

Keskeinen oppimiskokemus liittyi olemassa olevan infrastruktuurin merkitykseen. Projekti konkretisoi, kuinka passiivinen kaapelointi ja sen dokumentointi vaikuttavat suoraan järjestelmän luotettavuuteen ja käyttöönoton sujuvuuteen. Kaapelointimittausten ja vianmäärityksen kautta kehittyi kyky arvioida mittaustuloksia suhteessa todellisiin käyttövaatimuksiin sekä tehdä perusteltuja päätöksiä infrastruktuurin hyödyntämisestä tai korjaamisesta.

Työ syvensi osaamista IP-pohjaisten valvontajärjestelmien suunnittelussa ja hallinnassa. VLAN-segmentointi, palomuuripolitiikat ja roolipohjainen käyttöoikeuksien hallinta osoittivat käytännössä, miten tietoturva ja toiminnallisuus voidaan yhdistää hallituksi kokonaisuudeksi. Demoympäristön hyödyntäminen ennen lopullista käyttöönottoa korosti iteratiivisen suunnittelun ja riskienhallinnan merkitystä infrastruktuuriprojekteissa.

Lisäksi projekti kehitti projektinhallinnallisia valmiuksia, kuten vaiheistusta, aikataulutusta ja teknisen dokumentaation tuottamista osana järjestelmän elinkaarta. Työssä omaksutut

toimintamallit ja periaatteet ovat sovellettavissa vastaaviin verkko- ja valvontajärjestelmähankkeisiin ja tukevat ammatillista kehittymistä tietoverkko- ja tietoturva-alalla.

9 Yhteenveto ja pohdinta

Tämän opinnäytetyön tavoitteena oli suunnitella ja toteuttaa yritysympäristöön IP-pohjainen kameravalvontajärjestelmä, joka täyttää toiminnalliset, tekniset ja lainsäädännölliset vaatimukset. Työssä yhdistettiin tekninen mitoitus, käytännön toteutus ja järjestelmän arviointi todellisessa käyttöympäristössä siten, että lopputuloksena syntyi hallittava ja dokumentoitu kokonaisratkaisu.

Asetetut tavoitteet saavutettiin. Järjestelmä on osoittautunut käytännössä toimivaksi ja luotettavaksi, ja sen kriittiset toiminnot, kuten paikallinen tallennus, verkkoyhteys ja PoE-virransyöttö, ovat toimineet vakaasti. Verkkoarkkitehtuuri, VLAN-segmentointi ja palomuuripolitiikat tukevat tietoturvaa ja ylläpidettävyyttä, ja tallennusratkaisu vastaa mitoitusvaiheessa asetettuja vaatimuksia. Ratkaisu toteutettiin sovellettavaa kameravalvontaa koskevaa lainsäädäntöä ja tietosuojaperiaatteita noudattaen, mikä on olennainen osa nykyaikaista valvontajärjestelmää.

Työn aikana kävi ilmi, että olemassa olevan infrastruktuurin kunto ja dokumentoinnin taso vaikuttavat merkittävästi projektin sujuvuuteen ja lopputuloksen laatuun. Puutteellinen kaapelointidokumentaatio ja tekniset rajoitteet lisäsivät käyttöönoton työmäärää, mutta järjestelmällisillä mittauksilla, vianmäärityksellä ja selkeällä dokumentoinnilla nämä riskit pystyttiin hallitsemaan. Lopputuloksena syntynyt dokumentaatio tukee järjestelmän pitkäaikaista ylläpitoa ja mahdollistaa hallitut laajennukset.

Jatkokehityksen näkökulmasta järjestelmää voidaan laajentaa kasvattamalla tallennuskapasiteettia, lisäämällä kameroita tai kehittämällä runkoverkkoa esimerkiksi kuitupohjaiseksi. Lisäksi älykkäiden analytiikka- ja tapahtumapohjaisten toimintojen hyödyntämistä voidaan lisätä, kuitenkin lainsäädännön ja tietosuojan asettamat rajat huomioiden.

Laajemmassa tarkastelussa työ osoittaa, että yritysympäristön kameravalvonta ei ole pelkästään tekninen toteutus, vaan osa kokonaisvaltaista riskienhallintaa ja turvallisuuskulttuuria. Huolellisesti suunniteltu, mitoitettu ja dokumentoitu järjestelmä parantaa toiminnan läpinäkyvyyttä ja organisaation valmiutta reagoida poikkeustilanteisiin. Tekninen toteutus ei yksin ratkaise kaikkia turvallisuushaasteita, mutta järjestelmällinen ja eettisesti kestävä lähestymistapa vahvistaa toimintaympäristön turvallisuutta pitkäjänteisesti.

Lähteet

Axis Communications. 2007. IP-Surveillance Design Guide: Setting up an IP-Surveillance system using Axis cameras and AXIS Camera Station software. Viitattu 9.2.2026. Saatavissa: https://www.omegacubed.net/axis/axis_general_pdf/omegacubed.net_setting_up_ip_surveillance.pdf

Axis Communications. 2021. Edge storage – Flexible and reliable recording solutions. White paper. Viitattu 9.2.2026. Saatavissa: https://www.axis.com/files/whitepaper/wp_edge_storage_en_2112.pdf

EDPB (European Data Protection Board). 2020. Guidelines 3/2019 on processing of personal data through video devices. Viitattu 18.9.2025. Saatavissa: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

Elsevier B.V. 2026. Broadcast Domain. ScienceDirect Topics. Viitattu 9.2.2026. Saatavissa: https://www.sciencedirect.com/topics/computer-science/broadcast-domain

EtherWAN Systems. 2023. Implementing Quality of Service: Prioritizing Network Traffic. Viitattu 11.1.2026. Saatavissa: https://www.etherwan.com/support/featured-articles/implementing-quality-service-prioritizing-network-traffic

European Commission. 2025. Guidelines on prohibited AI practices. Viitattu 4.2.2025. Saatavissa: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act

European Union. 2016. Regulation (EU) 2016/679 (General Data Protection Regulation). EUR-Lex. Viitattu 18.9.2025. Saatavissa: https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Union. 2024. Regulation (EU) 2024/1689 (Artificial Intelligence Act). EUR-Lex. Viitattu 18.9.2025. Saatavissa: https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Fluke Networks. 2025. Attenuation (Insertion Loss) Measurement and Testing – DTX CableAnalyzer. Viitattu 1.2.2026. Saatavissa: https://www.flukenetworks.com/knowledge-base/dtx-cableanalyzer/attenuation-insertion-loss-measurement-and-testing-dtx

Fluke Networks. 2025. NEXT (Near-End Crosstalk) Troubleshooting. Viitattu 1.2.2026. Saatavissa: https://www.flukenetworks.com/support/knowledge-base/dtx-cableanalyzertm/next-near-end-crosstalk-troubleshooting

Fluke Networks. 2025. Power Sum NEXT (PS NEXT). Viitattu 1.2.2026. Saatavissa: https://www.flukenetworks.com/knowledge-base/dtx-cableanalyzer/power-sum-next-ps-next

Fluke Networks. 2025. Return Loss Measurement and Testing. Viitattu 1.2.2026. Saatavissa: https://www.flukenetworks.com/knowledge-base/dtx-cableanalyzer/return-loss-measurement-and-testing

Fluke Networks. 2025. Attenuation to Crosstalk Ratio Near-End (ACR-N) – DTX CableAnalyzer. Viitattu 1.2.2026. Saatavissa: https://www.flukenetworks.com/knowledge-base/dtx-cableanalyzer/attenuation-crosstalk-ratio-near-end-acr-n-dtx-cableanalyzer

Fluke Networks. 2025. ACR-F, formally known as Equal Level Far End Crosstalk (ELFEXT). Viitattu 1.2.2026. Saatavissa: https://www.flukenetworks.com/knowledge-base/dtx-cableanalyzer/acr-f-formally-known-equal-level-far-end-crosstalk-elfext

Fortinet. 2025. Understanding IP Surveillance Camera Bandwidth. White paper. Viitattu 31.1.2026. Saatavissa: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-ip-surveillance-camera.pdf

Fortinet. 2026. What Is Quality of Service (QoS) In Networking? CyberGlossary. Viitattu 31.1.2026. Saatavissa: https://www.fortinet.com/resources/cyberglossary/qos-quality-of-service

Huawei Technologies. 2024. What Is Virtual Local Area Network (VLAN). IP Encyclopedia. Viitattu 31.1.2026. Saatavissa: https://info.support.huawei.com/info-finder/encyclopedia/en/VLAN.html

International Organization for Standardization (ISO). 1994. ISO/IEC 7498-1: Information technology – Open Systems Interconnection – Basic Reference Model. Geneva: ISO/IEC. Viitattu 20.1.2026. Saatavissa rajoitetusti.

Internet Engineering Task Force (IETF). 1981. RFC 791: Internet Protocol. Viitattu 20.1.2026. Saatavissa: https://www.rfc-editor.org/rfc/rfc791

Internet Engineering Task Force (IETF). 1997. RFC 2131: Dynamic Host Configuration Protocol. Viitattu 20.1.2026. Saatavissa: https://www.rfc-editor.org/rfc/rfc2131

Laki yksityisyyden suojasta työelämässä 759/2004. Finlex. Viitattu 18.9.2025. Saatavissa: https://www.finlex.fi/fi/lainsaadanto/2004/759

Lammle, T. 2017. CCNA Routing and Switching: Complete Review Guide. E-kirja. Indianapolis: Sybex. Viitattu 20.1.2026.

Li, Y. & Zhu, Z. 2020. Adaptive maintain power signature scheme for power over ethernet system. IET Power Electronics. Viitattu 20.1.2026. Saatavissa rajoitetusti.

Lubobya, S. C., Dlodlo, M. E.-H. & de Jager, G. 2018. Mesh IP Video Surveillance Systems Model Design and Performance Evaluation. Wireless Personal Communications. E-kirja. Viitattu 1.2.2026. Saatavissa rajoitetusti.

Microsoft. 2009. What Is Unicast IPv4 Routing? Viitattu 9.2.2026. Saatavissa: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc736574(v=ws.10)

Rikoslaki 39/1889. Finlex. Viitattu 18.9.2025. Saatavissa: https://www.finlex.fi/fi/lainsaadanto/1889/39-001

TeleDynamics. 2023. How to leverage multicast for your VoIP, UC & video systems. Viitattu 11.1.2026. Saatavissa: https://info.teledynamics.com/blog/how-to-leverage-multicast-for-your-voip-uc-video-systems

Tietosuojalaki 1050/2018. Finlex. Viitattu 18.9.2025. Saatavissa: https://www.finlex.fi/fi/lainsaadanto/2018/1050

Tietosuojavaltuutetun toimisto. 2020. Työelämän tietosuojan käsikirja. Viitattu 18.9.2025. Saatavissa: https://tietosuoja.fi/documents/6927448/8214540/Ty%C3%B6el%C3%A4m%C3%A4n+tietosuojan+k%C3%A4sikirja+2020-+Tietosuojavaltuutetun+toimisto.pdf

Tietosuojavaltuutetun toimisto. 2023. Kameravalvonta – usein kysyttyä. Viitattu 18.9.2025. Saatavissa: https://tietosuoja.fi/usein-kysyttya-kameravalvonta

Ubiquiti Inc. 2026. Intro to Networking – Power Over Ethernet (PoE). Viitattu 9.2.2026. Saatavissa: https://help.ui.com/hc/en-us/articles/360015399993-Intro-to-Networking-Power-Over-Ethernet-PoE

Ubiquiti Inc. 2024a. UniFi Protect G6 Bullet – Technical Specifications. Viitattu 20.1.2026. Saatavissa: https://eu.store.ui.com/eu/en/category/all-cameras-nvrs/products/uvc-g6-bullet

Ubiquiti Inc. 2024b. UniFi Protect G6 Dome – Technical Specifications. Viitattu 20.1.2026. Saatavissa: https://eu.store.ui.com/eu/en/category/all-cameras-nvrs/products/uvc-g6-dome

Ubiquiti Inc. 2024c. UniFi Protect G6 Turret – Technical Specifications. Viitattu 20.1.2026. Saatavissa: https://eu.store.ui.com/eu/en/category/all-cameras-nvrs/products/uvc-g6-turret

Ubiquiti Inc. 2024d. UniFi Dream Machine Special Edition – Technical Specifications. Viitattu 20.1.2026. Saatavissa: https://eu.store.ui.com/eu/en/category/cloud-gateways/products/udm-se

Ubiquiti Inc. 2026. UniFi Protect Cameras – AI Detections and Facial Recognition. Viitattu 1.2.2026. Saatavissa: https://help.ui.com/hc/en-us/articles/360058867233-UniFi-Protect-Cameras-AI-Detections-and-Facial-Recognition